# DBAT Level 2

# Online Safety Policy

## St Peter's Academy

## March 2023

# Contents

# Development / Monitoring / Review of this Policy

This Online Safety policy has been developed in consultation with

- Headteacher / Senior Leaders
- Online Safety Officer (Headteacher)
- Staff – including Teachers, Support Staff
- Technical support staff
- Academy Council Members

# Schedule for Development / Monitoring / Review

| | |
|---|---|
| This Online Safety policy was approved by the Academy Council on: | March 2022 |
| The implementation of this Online Safety policy will be monitored by the: | Headteacher / IT leader |
| Monitoring will take place at regular intervals: | Annually |
| The Academy Council will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | Annually |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | March 2023 |
| Should serious online safety incidents take place, the following external persons / agencies should be informed: | Trust Safeguarding Officer, Academy Group Officials, LADO, Police |

The academy will monitor the impact of the policy using: (delete / add as relevant)

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

## Scope of the Policy

This policy applies to all members of the academy community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of academy.

## Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy

## Governors / Board of Directors:

The Academy Council is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Safeguarding Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Academy Council has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs

- reporting to relevant Governors / Board / Committee / meeting

## Headteacher / Principal and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the academy community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in academy who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

## Online Safety Coordinator / Officer -Designated safeguarding lead:

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the academy online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with academy technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

## Network Manager / Technical staff:

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements and any Local Authority / Academy Group / other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

## Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current academy Online Safety Policy and practices
- they have read, understood, and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction

- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official academy systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other academy activities (where allowed) and implement current policies about these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Designated Safeguarding Lead / Designated Person / Officer

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

## Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the academy this group may be part of the safeguarding group.  The group will also be responsible for regular reporting to the Directors.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator / Officer (or another relevant person, as above) with:

- the production / review / monitoring of the academy Online Safety Policy / documents.
- the production / review / monitoring of the academy filtering policy (if the academy chooses to have one) and requests for filtering changes.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Pupils from the School Council provide feedback to the Online safety co-ordinator (Headteacher) and their comments are fed back to the online safety group, comprising staff, parents/carers, and a member of the Academy Council.

## Students / Pupils:

- are responsible for using the academy digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of academy and realise that the academy's Online Safety Policy covers their actions out of academy, if related to their membership of the academy

## Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at academy events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- their children's personal devices in the academy (where this is allowed)

## Community Users

Community Users who access academy systems / website / Learning Platform as part of the wider academy provision will be expected to sign a Community User AUA before being provided with access to academy systems. (A Community Users Acceptable Use Agreement Template can be found in the appendices.)

# Policy Statements

## Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the academy's / academy's online safety provision. Children and young people need the help and support of the academy to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside academy.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g., Safer Internet Day

- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/  http://www.childnet.com/parents-and-carers

## Education – The Wider Community

The academy will provide opportunities for local community groups / members of the community to gain from the academy's / academy's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy, and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision where suitable

## Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

## Training – Governors / Directors

Governors / Directors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered through:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g., SWGfL) / Educare training
- Participation in academy training / information sessions for staff or parents.

## Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities

Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements:

- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- Users will be provided with a username and secure password by the technical support. Users are responsible for the security of their username and password and will be required to change their password at directed by the technical support company.
- The “master / administrator” passwords for the academy ICT system, used by the Network Manager (or another person) must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place.
- The Estates and Facilities business partner is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place by the Academy Trust to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The academy has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- Technical support staff regularly monitor and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Online safety leader/ headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data. These are tested regularly by the technical support company. The academy infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the academy systems using a 'Guest Login'.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on academy devices that may be used out of academy: Devices are only to be used for academy related work.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on academy devices: Permission should always be sought from the technical support provider.

• An agreed policy is in place regarding the use of removable media (e.g., memory sticks / CDs / DVDs) by users on academy devices: Memory sticks should not be used. Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.

## Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be academy owned/provided or personally owned and might include smartphone, tablet, notebook / laptop, or other technology that usually has the capability of utilizing the academy's wireless network. The device then has access to the wider internet which may include the academy's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a academy context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant academy polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the academy's Online Safety education programme.

- The academy Acceptable Use Agreements for staff, pupils/students and parents/ carers will give consideration to the use of mobile technologies
- The academy allows:

| | Academy Devices | | | Personal Devices | | |
|---|---|---|---|---|---|---|
| | Academy owned for single user | Academy owned for multiple users | Authorised device[1] | Student owned | Staff owned | Visitor owned |
| Allowed in academy | Yes | Yes | Yes | No[2] | Yes | Yes |
| Full network access | Yes | Yes | Yes | No | No | No |
| Internet only | | | | No | Yes | Yes[3] |
| No network access | | | | No | | No |

[1] Authorised device – purchased by/for the pupil/family through a academy-organised scheme. This device may be given full access to the network as if it were owned by the academy.

[2] If parents wish children to have mobile phones on them for unaccompanied journeys to/ from academy, they complete a permission form. If permission is granted, phones are to be handed in to their class teacher at the start of the day and only collected when leaving academy.

[3] At the discretion / with permission of the Online safety leader / Headteacher.

Aspects that the academy may wish to consider and be included in their Online Safety Policy, Mobile Technologies Policy or Acceptable Use Agreements:

Academy owned / provided devices:

- Who they will be allocated to
- Where, when, and how their use is allowed – times / places / in academy / out of academy
- If personal use is allowed
- Levels of access to networks / internet (as above)
- Management of devices / installation of apps / changing of settings / monitoring
- Network / broadband capacity
- Technical support
- Filtering of devices
- Access to cloud services
- Data Protection
- Taking / storage / use of images
- Exit processes – what happens to devices / software / apps / stored data if user leaves the academy
- Liability for damage
- Staff training

Personal devices:

- Staff may use personal devices in the school for personal use and for academy business
- They will have access to the Internet but not the network.
- No technical support is available for personal equipment
- Filtering of the internet connection to these devices
- Data Protection
- Employers have the right to take, examine and search users' devices in the case of misuse
- Images may not be taken  or stored on personal devices.
- DBAT and the academy will not be liable for loss/damage or malfunction following access to the network.
- Identification / labelling of personal devices
- Visitors will be informed about academy requirements on their first visit to the school

- Education about the safe and responsible use of mobile devices is included in the academy Online Safety education programmes.

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the academy website / social media / local press (covered as part of the Parents / Carers Acceptable Use Agreement in the appendix)
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil, parents or carers.

# Data Protection

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant, and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out

- It has clear and understood arrangements for the security, storage, and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing, and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with academy policy (below) once it has been transferred or its use is complete

Memory sticks should not be used to transfer any pupil / personal information.

# Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the academy currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

| | Staff & other adults | | | Pupils | | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to the Academy | X | | | | | | x | |
| Use of mobile phones in lessons | | | | x | | | | x |
| Use of mobile phones in social time | | x | | | | | | x |
| Taking photos on mobile phones / cameras | | | | x | | | | x |
| Use of other mobile devices e.g. tablets, gaming devices | | | | x | | | | x |
| Use of personal email addresses in Academy , or on academy network | | x | | | | | | x |
| Use of academy email for personal emails | | | | x | | | | x |

|  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| Use of messaging apps |  | x |  |  |  |  |  | x |
| Use of social media |  | x |  |  |  |  |  | x |
| Use of blogs |  | x |  |  |  |  |  | x |

When using communication technologies, the academy considers the following as good practice:

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the academy email service / platforms to communicate with others when in academy, or on / academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class email addresses/logins may be used, while students / pupils at KS2 may be provided with individual academy email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

# Social Media - Protecting Professional Identity

All academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race, or disability or who defame a third party may render the academy or local authority / academy group liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The Academy provides the following measures to ensure reasonable steps are in place to minimize risk of harm to pupils, staff, and the academy through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Academy staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or academy staff
- They do not engage in online discussion on personal matters relating to members of the academy community
- Personal opinions should not be attributed to the academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official academy social media accounts are established, there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the academy are outside the scope of this policy
- Where excessive personal use of social media in academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The Academy permits reasonable and appropriate access to private social media sites during planned lunch breaks.

Monitoring of Public social media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the academy
- The academy should effectively respond to social media comments made by others according to a defined policy or process

The academy's use of social media for professional purposes will be checked regularly by the academy business partner (E and F) to ensure compliance with the academy policies.

## Unsuitable / inappropriate activities

Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g., cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a academy /academy context, either because of the age of the users or the nature of those activities.

The academy believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in / or outside the academy when using academy equipment or systems. The academy policy restricts usage as follows:

<table>
<tr><th colspan="2">User Actions</th><th>Acceptable</th><th>Acceptable at certain times</th><th>Acceptable for nominated users</th><th>Unacceptable</th><th>Unacceptable and illegal</th></tr>
<tr><td rowspan="9">Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</td><td>Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978</td><td></td><td></td><td></td><td></td><td>X</td></tr>
<tr><td>Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.</td><td></td><td></td><td></td><td></td><td>X</td></tr>
<tr><td>Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008</td><td></td><td></td><td></td><td></td><td>X</td></tr>
<tr><td>Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986</td><td></td><td></td><td></td><td></td><td>X</td></tr>
<tr><td>Pornography</td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td>Promotion of any kind of discrimination</td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td>threatening behaviour, including promotion of physical violence or mental harm</td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td>Promotion of extremism or terrorism</td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td>Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute</td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td colspan="2">Using academy systems to run a private business</td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td colspan="2">Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy</td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td colspan="2">Infringing copyright</td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td colspan="2">Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)</td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td colspan="2">Creating or propagating computer viruses or other harmful files</td><td></td><td></td><td></td><td>X</td><td></td></tr>
</table>

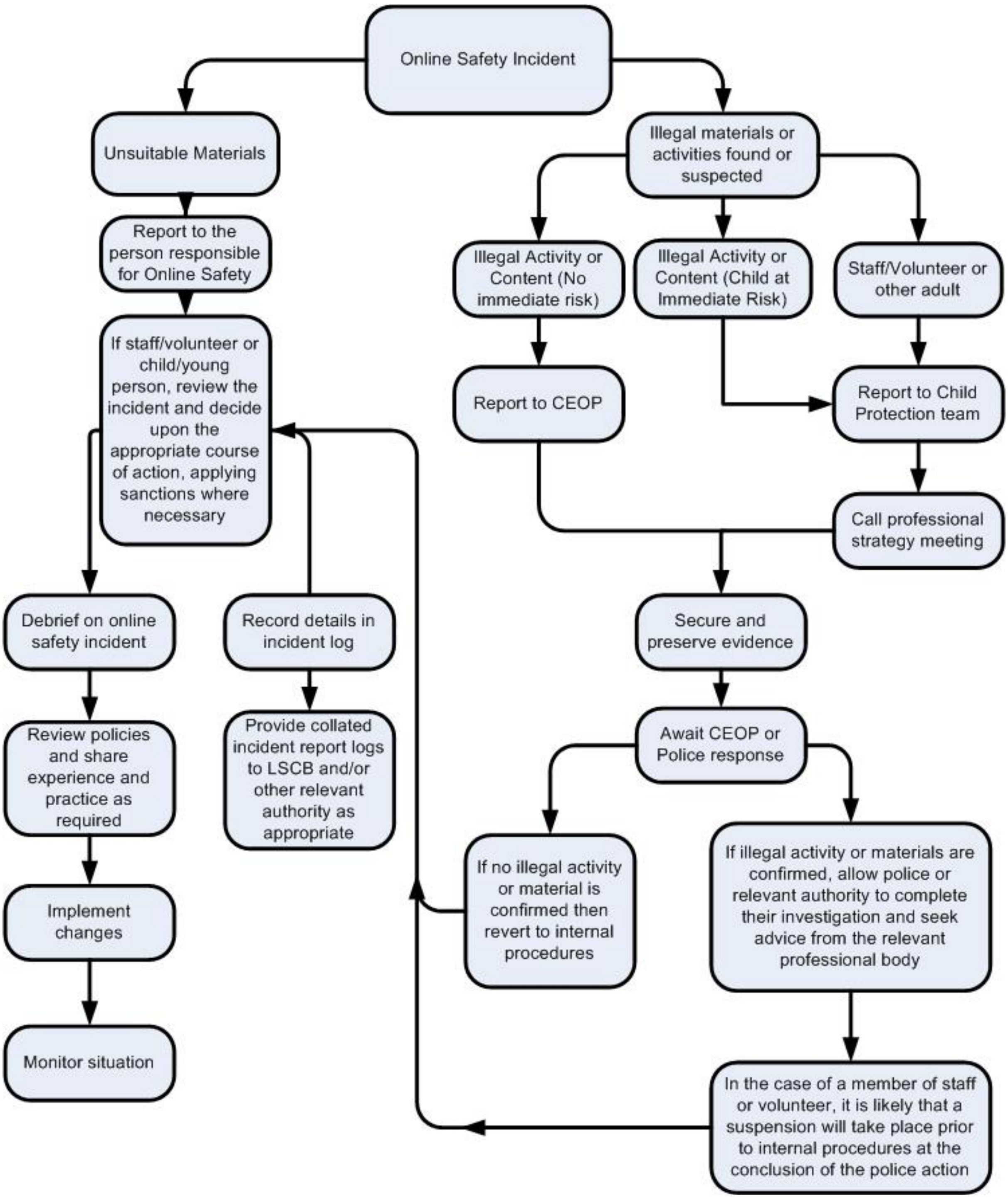
| | | | | | |
|---|---|---|---|---|---|
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | X | |
| On-line gaming (educational) | | x | | | |
| On-line gaming (non-educational) | | x | | | |
| On-line gambling | | | | x | |
| On-line shopping / commerce | | | x | | |
| File sharing | x | | | | |
| Use of social media | | x | | | |
| Use of messaging apps | | x | | | |
| Use of video broadcasting e.g., YouTube | x | | | | |

## Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

# Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

## Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action

- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism

    - other criminal conduct, activity, or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

# Academy Actions & Sanctions

It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows and could include:

| | Actions / Sanctions | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Pupils Incidents** | Refer to class teacher | Refer to Head of Key Stage | Refer to Headteacher / Principal | Refer to Police | Refer to technical support staff for action re filtering / security etc. | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction e.g. exclusion |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | X | X | X | X | X | X | X | X | X |
| Unauthorised use of non-educational sites during lessons | X | X | X | | | X | X | X | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device | X | X | X | X | | X | X | X | X |
| Unauthorised / inappropriate use of social media / messaging apps / personal email | X | X | X | X | X | X | X | X | X |
| Unauthorised downloading or uploading of files | X | X | X | X | X | X | X | X | X |
| Allowing others to access academy network by sharing username and passwords | X | X | X | | X | X | X | X | X |
| Attempting to access or accessing the academy network, using another student's / pupil's account | X | X | X | | X | X | X | X | X |
| Attempting to access or accessing the academy network, using the account of a member of staff | X | X | X | | X | X | X | X | X |
| Corrupting or destroying the data of other users | X | X | X | | X | X | X | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | X | | X | X | X | X |
| Continued infringements of the above, following previous warnings or sanctions | X | X | X | X | | X | X | X | X |
| Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy | X | X | X | | X | X | X | X | X |
| Using proxy sites or other means to subvert the academy's filtering system | X | X | X | | X | X | X | X | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | X | X | X | X | X | X | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X | X | X | X | X | X | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | X | X | X | | X | X | X | X | |

| Staff Incidents | Actions / Sanctions | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Refer to line manager | Refer to Headteacher | Refer to HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | Warning | Suspension | Disciplinary action |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | | X | X | X | | X | X | X |
| Inappropriate personal use of the internet / social media / personal email | | X | X | | | X | X | X |
| Unauthorised downloading or uploading of files | | X | X | | X | X | X | X |
| Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person's account | | X | X | X | X | X | X | X |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | | X | X | | | X | X | X |
| Deliberate actions to breach data protection or network security rules | | X | X | X | X | X | X | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | X | X | X | X | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | X | X | X | | X | X | X |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils | | X | X | X | X | X | X | X |
| Actions which could compromise the staff member's professional standing | | X | X | | | X | X | X |
| Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy | | X | X | | | X | X | X |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Using proxy sites or other means to subvert the academy's filtering system | | X | X | | X | X | X | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | X | X | X | X | X | X | X |
| Deliberately accessing or trying to access offensive or pornographic material | | X | X | X | X | X | X | X |
| Breaching copyright or licensing regulations | | X | X | | X | X | X | X |
| Continued infringements of the above, following previous warnings or sanctions | | X | X | | X | X | X | X |

# Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy

## Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this Academy Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2016. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

# Appendices

# St. Peter’s Acceptable Internet Use Policy

Dear Parents and Carers,

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

At St. Peter’s, we take the safe use of all equipment and online safety very seriously, so the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. We will also educate pupils so that they are aware of how to keep themselves safe.

We would be grateful if you could discuss these agreements with your child and return the back sheet to their class teacher.

Many thanks for your support in this important area,

Mark Everett (Headteacher)

# Reception and KS1 Pupils – Rules for Safe Internet Use

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will tell a teacher if something is broken
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen

- I know that if I break the rules I might not be allowed to use a computer / tablet

# **Parent / Carers Acceptable Internet Use Policy**

Parents play an integral role in supporting the school to ensure that pupils use the internet in a responsible way, so we ask you to support us by agreeing to the following:

- I agree that I have read and understood the school rules for Responsible internet Use and give permission for my child to access the Internet.
- I agree to support my child to follow these rules, both in school and at home.
- I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.
- I understand that the school cannot ultimately be held responsible for the nature or content of materials accessed through the internet by my child.
- I agree that the school is not liable for any damages arising from use of devices such as computers or tablets at school.
- I understand that should my child bring a personal device, such as a mobile phone, into school without permission then it will be confiscated and I will be required to collect it.
- I understand that the school will not be held responsible for loss or damages of any devices brought in to school by my child without permission.
- I understand that there will be consequences for my child if they break the school rules and I will support the school in implementing these.
- I agree to support the school by discouraging my child from accessing social media sites, films and games that are not age appropriate.
- I agree that, if selected, my child's work may be published on the school website.
- I  agree that images, sound files and video that include my child may be published subject to the school rules and that this content will not clearly identify individuals and that full names will not be used anywhere in association with photographs.
- I agree that should I take pictures, videos or sound recordings at school events, of any child other than my own, I will not share them on any social media sites.
- I agree that I will never share any pictures, videos or sound recording of any members of staff employed by the school on social media sites without their permission.
- I agree that I will not publish any grievances that I may have about staff or pupils at the school on social media. I will follow the schools Complaints Procedure or I will discuss them with the relevant member of staff instead.

**Please complete this section to show that your child has had the Acceptable Internet Use Agreement read to them and that they understand and agree to the rules included in it. If you do not sign and return this agreement, access will not be granted to all aspects of the school systems and devices.**

## Reception and KS1 Pupil Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Internet Use Agreement, which it is attached.

I have shared this information with my child and they have agreed to do their best to follow the school rules. They understand the consequences should they break them.

Name of pupil: ........................................................................

Signed (parent):.......................................................................

## Parent / Carer Acceptable Internet Use Agreement Form

This form relates to the Parent Agreement, which is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Parent Acceptable Internet Use Agreement. If you do not sign and return this agreement, access will not be granted to all aspects of the school systems.

I have read and understood the above and agree to follow these guidelines:

Name of Parent or Carer: ........................................................................................................

Signed (parent) ........................................................................................................

Date: ........................................................................................................

# St. Peter's Acceptable Internet Use Policy

Dear Parents and Carers,

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

At St. Peter's, we take the safe use of all equipment and  online safety very seriously, so the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems.  We will also educate pupils so that they are aware of how to keep themselves safe.

We would be grateful if you could discuss these agreements with your child/ren and return the back sheet to their class teacher.

Many thanks for your support in this important area,

Mark Everett (Headteacher)

# KS2 Pupils – Rules for Acceptable Internet Use

This Acceptable Internet Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for **educational, personal and recreational use;**
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk. Pupils will have good access to digital technologies to enhance their learning and we will, in return, expect them to agree to be responsible users.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.).
- I will not arrange to meet people offline that I have communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages, or anything that makes me feel uncomfortable, to an appropriate adult when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for online gaming, internet shopping, file sharing or video broadcasting (e.g. YouTube) unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc) in school with the permission of an adult. Devices may be confiscated and my parent or guardian will be asked to collect them should you bring them to school without permission.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails on any school device.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites in school.

When using the internet for research or recreation, I recognise that.

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Internet Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network, internet, suspensions, my parents being contacted and, in the event of illegal activities, involvement of the police.

# Parent / Carers Acceptable Internet Use Policy

Parents play an integral role in supporting the school to ensure that pupils use the internet in a responsible way, so we ask you to support us by agreeing to the following:

- I agree that I have read and understood the school rules for Responsible Internet Use and give permission for my child to access the internet.
- I agree to support my child to follow these rules, both in school and at home.
- I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.
- I understand that the school cannot ultimately be held responsible for the nature or content of materials accessed through the internet by my child.
- I agree that the school is not liable for any damages arising from use of devices such as computers or tablets at school.
- I understand that should my child bring a personal device, such as a mobile phone, into school without permission then it will be confiscated and I will be required to collect it.
- I understand that the school will not be held responsible for loss or damages of any devices brought in to school by my child without permission.
- I understand that there will be consequences for my child if they break the school rules and I will support the school in implementing these.
- I agree to support the school by discouraging my child from accessing social media sites, films and games that are not age appropriate.
- I agree that, if selected, my child's work may be published on the school website.
- I agree that images, sound files and video that include my child may be published subject to the school rules and that this content will not clearly identify individuals and that full names will not be used anywhere in association with photographs.
- I agree that should I take pictures, videos or sound recordings at school events, of any child other than my own, I will not share them on any social media sites.
- I agree that I will never share any pictures, videos or sound recording of any members of staff employed by the school on social media sites without their permission.
- I agree that I will not publish any grievances that I may have about staff or pupils at the school on social media. I will follow the schools Complaints Procedure or I will discuss them with the relevant member of staff instead.

**Please complete this section to show that you have read, understood and agree to the rules included in the Acceptable Internet Use Agreement. If you do not sign and return this agreement, access will not be granted to all aspects of the school systems and devices.**

## KS2 Pupil Acceptable Internet Use Agreement Form

This form relates to the pupil Acceptable Internet Use Agreement, to which it is attached.

I have read, understood and agree to follow the Acceptable Internet Use Agreement.

Name of Pupil: ……………………………………………………………………

Class: ……………………………………………………………………

Date: ……………………………………………………………………

## Parent / Carer Acceptable Internet Use Agreement Form

This form relates to the Parent Agreement, which is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Parent Acceptable Internet Use Agreement. If you do not sign and return this agreement, access will not be granted to all aspects of the school systems.

I have read and understood the above and agree to follow these guidelines:

Name of Parent or Carer: ……………………………………………………………………

Signed: ……………………………………………………………………

Date: ……………………………………………………………………

# Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of academy. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the academy website and occasionally in the public media.

The academy will comply with the Data Protection Act and request parents / carers permission before taking images of members of the academy. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the academy to take and use images of their children and for the parents / carers to agree

## Digital / Video Images Permission Form

Parent / Carers Name: ------------------------------------------------------------

Student / Pupil Name: ------------------------------------------------------------

| | |
|---|---|
| As the parent / carer of the above student / pupil, I agree to the academy taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the academy. | Yes / No |
| I agree that if I take digital or video images at, or of – academy events which include images of children, other than my own, I will abide by these guidelines in my use of these images. | Yes / No |

Signed: ------------------------------------------------------------

Date: ------------------------------------------------------------

# Use of Cloud Systems Permission Form

Academies that use cloud hosting services may be required to seek parental permission to set up an account for pupils / students.

Google Apps for Education services – http://www.google.com/apps/intl/en/terms/education_terms.html requires a academy to obtain 'verifiable parental consent' for their children to be able to use these services. It is suggested that academys will incorporate this into their standard acceptable use consent forms sent to parents each year.

Academys will need to review and amend the section below, depending on which cloud hosted services are used.

The academy uses Google Apps for Education for pupils / students and staff. This permission form describes the tools and pupil / student responsibilities for using these services.

The following services are available to each pupil / student and hosted by Google as part of the academy's online presence in Google Apps for Education:

Mail - an individual email account for academy use managed by the academy

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Using these tools, pupils / students collaboratively create, edit and share files and websites for academy related projects and communicate via email with other pupils / students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of academy learning experiences, and working in small groups on presentations to share with others.

The academy believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent / Carers Name: ------------------------------------------------------------

Student / Pupil Name: ------------------------------------------------------------

As the parent / carer of the above student / pupil, I agree to my child using the academy using Google Apps for Education. Yes / No

Signed: ------------------------------------------------------------

Date: ------------------------------------------------------------

# Use of Biometric Systems

If the academy uses biometric systems (e.g. fingerprint / palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc. it must (under the "Protection of Freedoms" legislation) seek permission from a parent or carer. It is also recommended that they obtain this permission through the normal internet use permission / acceptable use agreement. Academys may therefore wish to add a section such as that below to this permission form.

The academy uses biometric systems for the recognition of individual children in the following ways (the academy should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or academy library) so nothing can be lost, such as a swipe card.

The academy has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a academy context.

No complete images of fingerprints / palms are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents / carers are asked for permission for these biometric technologies to be used by their child:

Parent / Carers Name: ----------------------------------------------------------------

Student / Pupil Name: ----------------------------------------------------------------

As the parent / carer of the above student / pupil, I agree to the academy using biometric recognition systems, as described above. I understand that the images cannot be used to create a whole fingerprint / palm print of my child and that these images will not be shared with anyone outside the academy. Yes / No

Signed: ----------------------------------------------------------------

Date: ----------------------------------------------------------------

# Staff (and Volunteer) Acceptable Use Policy Agreement Template

## Academy Policy

New technologies have become integral to the lives of children and young people in today's society, both within academys / academies and in their lives outside academy. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The academy will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

## Acceptable Use Policy Agreement

I understand that I must use academy systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of the academy digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of academy, and to the transfer of personal data (digital or paper based) out of academy
- I understand that the academy digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the academy. (academys should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of academy systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the academy website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in academy in accordance with the academy's policies.
- I will only communicate with students / pupils and parents / carers using official academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in academy, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the academy digital technology systems (both in and out of academy) and my own devices (in academy and when carrying out communications related to the academy) within these guidelines.

Staff / Volunteer Name: ----------------------------------------------------------

Signed: ----------------------------------------------------------

Date: ----------------------------------------------------------

# Acceptable Use Agreement for Community Users Template

This Acceptable Use Agreement is intended to ensure:

- that community users of academy digital technologies will be responsible users and stay safe while using these systems and devices
- that academy systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

## Acceptable Use Agreement

I understand that I must use academy systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the academy:

- I understand that my use of academy) systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into academy for any activity that would be inappropriate in a academy setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user’s files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.

- I will not publish or share any information I have obtained whilst in the academy on any personal website, social networking site or through any other means, unless I have permission from the academy.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a academy device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the academy has the right to remove my access to academy systems / devices

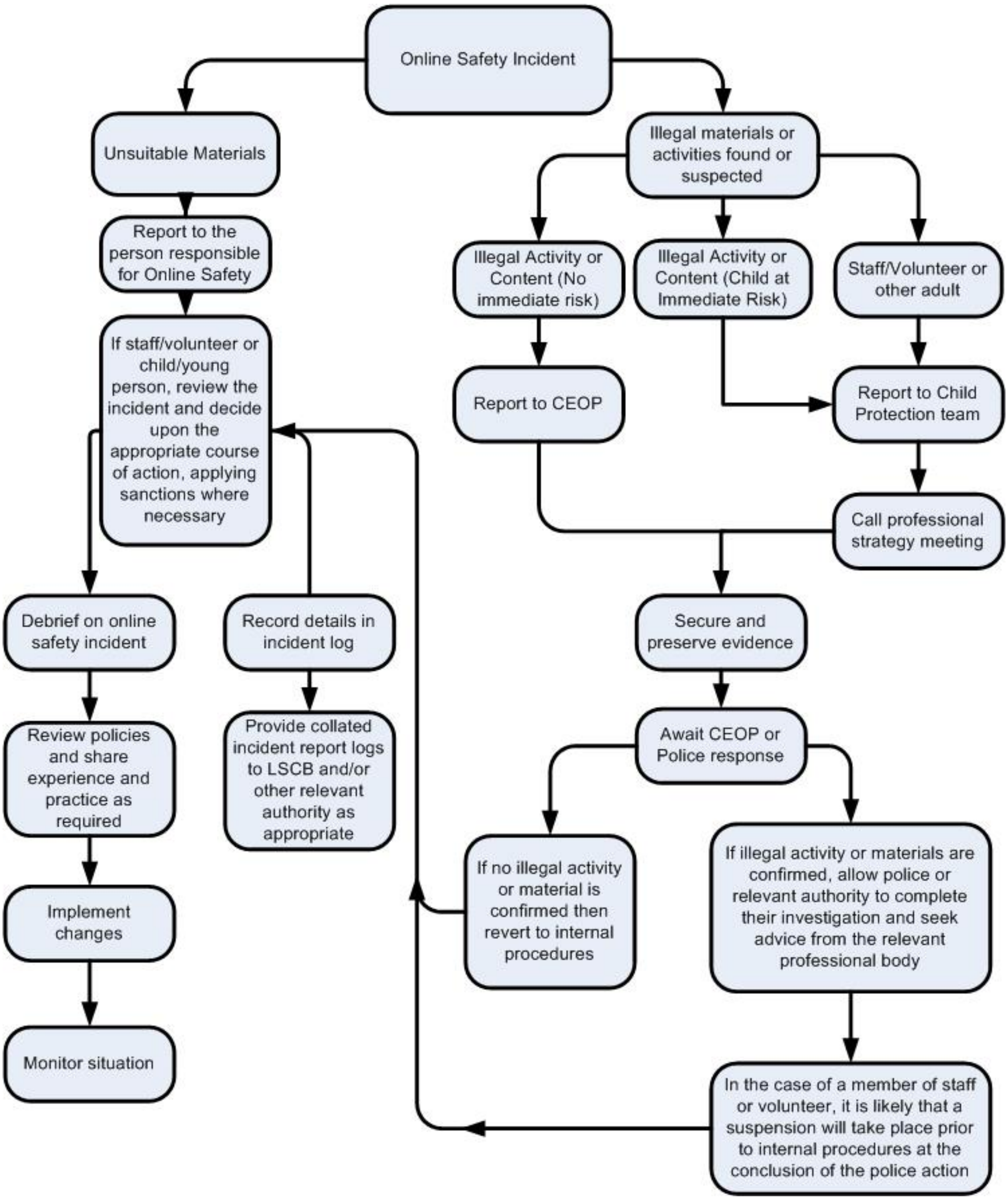
I have read and understand the above and agree to use the academy digital technology systems (both in and out of academy) and my own devices (in academy and when carrying out communications related to the academy) within these guidelines.

Name: ------------------------------------------------------------

Signed: ------------------------------------------------------------

Date: ------------------------------------------------------------

# Responding to incidents of misuse – flow chart



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

# Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: ------------------------------------------------------------------------------------

Date:

Reason for investigation:

Details of first reviewing person

Name:

Position:

Signature:

Details of second reviewing person

Name:

Position:

Signature:

## Name and location of computer used for review (for web sites)

| Web site(s) address / device | Reason for concern |
|---|---|
| | |
| | |
| | |
| | |
| | |

Conclusion and Action proposed or taken

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |

# Reporting Log

Group: ..........................................................................................

| Date | Time | Incident | Action Taken | | Incident Reported By | Signature |
|---|---|---|---|---|---|---|
| | | | What? | By Whom? | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Training Needs Audit Log

Group: ------------------------------------------------------------------------

| Relevant training the last 12 months | Identified Training Need | To be met by | Cost | Review Date |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Academy Technical Security Policy Template (including filtering and passwords)

### Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The academy will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the academy's policies).
- access to personal data is securely controlled in line with the academy's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of academy computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

## Responsibilities

The management of technical security will be the responsibility of Data Aspire.

## Technical Security

### Policy statements

The academy trust will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of academy academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the academy systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to academy technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The Estates and Facilities Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place (Academys / academies may wish to add details of the mobile device security procedures that are in use).
- Academy technical staff regularly monitor and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential technical incident to the Online Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed) using the DBAT incident form.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the academy system. (Username : Guest)

- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on academy devices by users, only by Dataspire.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on academy devices that may be used out of academy.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on academy devices. (DVDs are allowed , but not memory sticks)
- The academy infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.

# Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all academy technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

## Policy Statements

- All users will have clearly defined access rights to academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- All academy networks and systems will be protected by secure passwords that are regularly changed
- The “master / administrator” passwords for the academy systems, used by the technical staff must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place eg academy safe. Consideration should also be given to using two factor authentication for such accounts.
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- Passwords for new users, and replacement passwords for existing users will be allocated by Dataspire. Any changes carried out must be notified to the manager of the password security policy (above). Or:
- Passwords for new users and replacement passwords for existing users will be issued through an automated process.
- Users will change their passwords at regular intervals – as prescribed by Dataspire / DBAT
- Where passwords are set / changed manually requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (the academy will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)

## Staff Passwords

- All staff users will be provided with a username and password by (insert name or title / automated process) who / which will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of academy
- should be changed at least every 60 to 90 days, or as directed by DBAT / Daatapire.
- should not re-used for 6 months and be significantly different from previous passwords created by the same user. The last four passwords cannot be re-used.

### Student / Pupil Passwords

- All users will be provided with a username and password by Dataspire who / which will keep an up to date record of users and their usernames.
- Users will be required to change their password as directed by Dataspire.
- Students / pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

### Training / Awareness

Members of staff will be made aware of the academy's password policy:

- at induction
- through the academy's online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the academy's password policy:

- in lessons
- through the Acceptable Use Agreement

### Audit / Monitoring / Reporting / Review

The responsible person (Dataspire) will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ins
- Security incidents related to this policy

## Filtering

### Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this academy.

## Responsibilities

The responsibility for the management of the academy's filtering policy will be held by Dataspire They will manage the academy filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the academy filtering service must be requested and authourised by Dataspire.

- be logged in change control logs
- be reported to a second responsible person (
- be reported to the Online Safety Group every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to (insert title) any infringements of the academy's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

## Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the academy. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the academy to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the academy network, filtering will be applied that is consistent with academy practice.

- Either - The academy maintains and supports the managed filtering service provided by the Internet Service Provider.

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher / Principal (or other nominated senior leader).
- Mobile devices that access the academy internet connection (whether academy or personal devices) will be subject to the same filtering standards as other devices on the academy systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff / Headteacher . If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

### Education / Training / Awareness

Pupils / students will be made aware of the importance of filtering systems through the online safety lessons. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the academy's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

### Changes to the Filtering System

- If changes are required to the filtering system they should be made in writing /email to the technical support company (Dataspire)

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Headteacher will decide whether to make academy level changes (as above).

## Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The academy will therefore monitor the activities of users on the academy network and on academy equipment as indicated in the Academy Online Safety Policy and the Acceptable Use Agreement. Monitoring will take place by staff in lessons and Dataspire.

## Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to the academy by Dataspire to

- the second responsible person - DDSL
- Online Safety Group
- Online Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

## Further Guidance

Academys in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in academy, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, academys will be obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the academy or colleges IT system" however, academys will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

In response UKSIC produced guidance on – information on "Appropriate Filtering"

NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-academys/

Somerset Guidance for academys – this checklist is particularly useful where a academy uses external providers for its technical support / security: https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx

# Academy Personal Data Handling Policy Template

## Academy Personal Data Handling Policy

Recent publicity about data breaches suffered by organisations and individuals has made the area of personal data protection compliance a current and high profile issue for academys and other organisations. It is important that the academy has a clear and well understood personal data handling policy in order to avoid or at least minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- No academy or individual would want to be the cause of any data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Academys are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The academy will want to avoid the criticism and negative publicity that could be generated by any-personal data breach.
- The academy is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

It is a statutory requirement for all academys to have a Data Protection Policy.

Academys have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in academy but also from remote locations. Legislation covering the safe handling of this data is mainly the Data Protection Act 2018 ('the DPA'). Moreover, following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, Data Handling Procedures in Government. The latter stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in academies, it is critical that they adopt these procedures too.

It is important to stress that the Personal Data Handling Policy Template applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

## Introduction

Academys and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the academy community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the academy into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office ~~.~~ for the academy and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

The DPA lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines "Personal Data" as data which relate to a living individual who can be identified (http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions)

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines "Sensitive Personal Data" as personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

Guidance for organisations processing personal data is available on the Information Commissioner's Office website:
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

## Policy Statements

The academy will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section below)

## Personal Data

The academy and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the academy community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

## Responsibilities

The academy's Senior Information Risk Officer (SIRO) is Michelle Pennycott. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the academy's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The academy will identify Information Asset Owners (IAOsfor the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information as been amended or added to over time, and
- who has access to protected data and why.

Everyone in the academy has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

## Registration

The academy is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

## Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the academy will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through. Parents / carers of young people who are new to the academy will be provided with the privacy notice.

More information about the suggested wording of privacy notices can be found on the DfE website:

http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn. A copy of the guidance is also included as an appendix the end of this template policy. LA Academys are advised to contact their Local Authority for local versions of the Privacy Notice and to check for annual updates.

## Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

## Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

| Risk ID | Information Asset affected | Information Asset Owner | Protective Marking (Impact Level) | Likelihood | Overall risk level (low, medium, high) | Action(s) to minimise risk |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

| Government Protective Marking Scheme label | Impact Level (IL) | Applies to academys? |
|---|---|---|
| Not Protectively Marked | 0 | Will apply in academys |
| Protect | 1 or 2 | |
| Restricted | 3 | |
| Confidential | 4 | Will not apply in academys |
| Highly Confidential | 5 | |
| Top Secret | 6 | |

Most student / pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The academy will ensure that all academy staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g.. "Securely delete or shred this information when you have finished using it".

## Secure Storage of and access to data

The academy will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on academy equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and

- the data must be securely deleted from the device, in line with academy policy (below) once it has been transferred or its use is complete.

The academy  has clear policy and procedures for the automatic backing up, accessing and restoring all data held on academy systems, including off-site backups.

The academy has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The academy will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

(see appendix for further information and the ICO Guidance: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

As a Data Controller, the academy is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The academy recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

## Secure transfer of data and access out of academy

The academy recognises that personal data may be accessed by users out of academy, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of academy
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

## Disposal of data

The academy will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

## Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals. (insert name or title)

The audit logs will be kept to provide evidence of accidental or deliberate_data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The academy has a policy for reporting, managing and recovering from information risk incidents, which establishes.

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

## Use of technologies and Protective Marking

The following  provides a useful guide:

| | The information | The technology | Notes on Protect Markings (Impact Level) |
|---|---|---|---|
| Academy life and events | Academy terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events | Common practice is to use publically accessible technology such as academy websites or portal, emailed newsletters, subscription text services | Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |

| | | | |
|---|---|---|---|
| Learning and achievement | Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs. | Typically academys will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent. | Most of this information will fall into the PROTECT (Impact Level 2) category.<br>There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the academy may decide not to make this pupil / student record available in this way. |
| Messages and alerts | Attendance, behavioural, achievement, sickness, academy closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means. | Email and text messaging are commonly used by academys to contact and keep parents informed.<br>Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context. | Most of this information will fall into the PROTECT (Impact Level 1) category.<br>However, since it is not practical to encrypt email or text messages to parents, academys should not send detailed personally identifiable information.<br>General, anonymous alerts about academys closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |

# Appendices: Additional issues / documents related to Personal Data Handling in Academys:

## Use of Biometric Information

The Protection of Freedoms Act 2012, includes measures that will affect academys and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in academys and colleges under 18, they must obtain the written consent of a parent before they take and process their child's biometric data.
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 2018.
- They must provide alternative means for accessing services where a parent or pupil has refused consent.

New advice to academys will make clear that they will no longer be able to use pupils' biometric data without parental consent. The advice will come into effect from September 2013. Academys may wish to consider these changes when reviewing their Personal Data Handling Template. Academys may wish to incorporate the parental permission procedures into existing parental forms (eg AUP / Digital & Video Images permission form).

## Use of Cloud Services

Many academys now use cloud hosted services. This section is designed to help you to understand your obligations and help you establish the appropriate policies and procedures when considering switching from locally-hosted services to cloud-hosted services.

## What policies and procedures should be put in place for individual users of cloud-based services?

The academy is ultimately responsible for the contract with the provider of the system, so check the terms and conditions carefully; below is a list of questions that you may want to consider when selecting a cloud services provider; indeed you may want to contact any potential provider and ask them for responses to each of the following:

- How often is the data backed up?
- Does the service provider have a clear process for you to recover data?
- Who owns the data that you store on the platform?
- How does the service provider protect your privacy?

- Who has access to the data?
- Is personal information shared with anyone else? Look out for opt in/opt out features
- Does the service provider share contact details with third party advertisers? Or serve users with ads?
- What steps does the service provider take to ensure that your information is secure?
- Is encryption used? Is https used as default or is there an option to use this? Two step verification?
- How will your data be protected? Look out for features that will keep your information safe and secure including Anti-spam, Anti-Virus and Anti-malware…
- How reliable is the system? Look out for availability guarantees.
- What level of support is offered as part of the service? Look out for online and telephone support, service guarantees

SWGfL provides a useful summary of these issues in a document that has been written with the support of Google and Microsoft:

http://www.swgfl.org.uk/products-services/education/Resources/Cloud-Hosted-Services

The document focusses on Google Apps for Education and Microsoft 365, but poses important considerations if a academy is considering services from another provider.

## Parental permission for use of cloud hosted services

Academys that use cloud hosting services (eg.Google Aps for Education) may be required to seek parental permission to set up an account for pupils / students.

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a academy to obtain 'verifiable parental consent'. Normally, academys will incorporate this into their standard acceptable use consent forms sent to parents each year (see suggested wording on "Parent / Carer Acceptable Use Agreement Template").

A template form has been added to the Parents & Carers Acceptable User Template elsewhere in these Template Policies.

## Privacy and Electronic Communications

Academys should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

## Freedom of Information Act

All academys (including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy the academy should:

- Delegate to the Headteacher / Principal day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the academy's policy
- Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- Ensure that a well-managed records management and information system exists in order to comply with requests
- Ensure a record of refusals and reasons for refusals is kept, allowing the Academy Trust to review its access policy on an annual basis

## Model Publication Scheme

The Information Commissioners Office provides academys and academies with a model publication scheme which they should complete. This was revised in 2009, so any academy with a scheme published prior to then should review this as a matter of urgency. The academy's publication scheme should be reviewed annually.

Guidance on the model publication scheme can be found at:

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/

https://ico.org.uk/media/for-organisations/documents/1235/definition-document-academys-in-england.pdf

The Academys Model Publication Scheme Template is available from:

https://ico.org.uk/media/1278/academys_england_mps_final.doc

## Further Guidance

DfE guidance that is specific to Academies can be found at:

http://www.education.gov.uk/academys/leadership/typesofacademys/academies/open/a00205178/freedom-of-information-guide-for-academies

# Appendix - DfE Guidance on the wording of the Privacy Notice

PRIVACY NOTICE TEMPLATE

for

Pupils in Academys, Alternative Provision and Pupil Referral Units

and Children in Early Years Settings

(This is suggested text which can be amended to suit local needs and circumstances)

## Privacy Notice - Data Protection Act 2018

We St Peters C of E Academy are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous academy and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your academy is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

# Academy Policy Template: Electronic Devices - Searching & Deletion

The Education Act 2012, the basis of this template, sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.

No existing law or policy can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others. Anyone refraining from any such search, access or deletion when hindsight shows circumstances merit such actions may however be at significant risk and may put seriously at risk the wellbeing of children entrusted to their care. This template cannot therefore be relied on as justification for any act or lack of action by anyone – there is no substitute for the proper and well documented exercise of adequately informed professional judgement. .

It is for each academy's / academy's Headteacher / Principal and Governors / Directors to set, apply and monitor application of their own policies as guided by their head teacher, local authority and official guidance, especially if the academy is local authority maintained. This template is intended as an aide to this. South West Grid for Learning Trust does not and cannot accept and does not have responsibility for any academy's policy on this or any other matter.

Within this template, sections which include information or guidance are shown in BLUE. It is anticipated that academys will remove these sections from their completed policy documents, though this will be for the academy's relevant policy advisory group to recommend and for the head teacher and other governors to decide upon.

Where sections in the template are written in italics it is anticipated that academys would wish to consider whether or not to include that section or statement in their completed policy.

**Where sections are highlighted in BOLD text, it is the view of the SWGfL Online Safety Group that these ought to be an essential part of a academy online safety policy.**

The template uses the term students / pupils to refer to the children / young people attending the learning institution and the term Headteacher / Principal. Academys will need to choose which terms to use and delete the others accordingly.

## Introduction

The changing face of information technologies and ever increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to academys by statute to search pupils in order to maintain discipline and ensure safety. Academys are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the academy will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the academy with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the academy rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the academy rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the academy rules may only be searched for under these new powers if it has been identified in the academy rules as an item that can be searched for. It is therefore important that there is a academy policy which sets out clearly and unambiguously the items which:

- are banned under the academy rules; and
- are banned AND can be searched for by authorised academy staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the academy rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Head Teacher / Principal must publicise the academy behaviour policy, in writing, to staff, parents / carers and students / pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"

http://www.education.gov.uk/academys/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

## Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The Academy Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

## Responsibilities

The Headteacher / Principal is responsible for ensuring that the academy policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher/Principal will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: Headteacher, using a model policy provided by SWGFL and DBAT central team.

The Headteacher / Principal has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: Members of the SLT

The Headteacher / Principal may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

## Training / Awareness

Members of staff should be made aware of the academy's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the academy's online safety policy

Members of staff authorised by the Headteacher / Principal to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

# Policy Statements

## Search:

The academy Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils / students are allowed to bring mobile phones or other personal electronic devices to academy only with written permission and use them only within the rules laid down by the academy.

If pupils / students breach these roles:

Either:

The sanctions for breaking these rules will be: confiscation of mobile phone and returned at the end of the day to a parent.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the academy rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the academy rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a student / pupil is in possession of a prohibited item i.e. an item banned by the academy rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of pupils / students.)

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student / pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the student / pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student/ pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a student / pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the student/ pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student / pupil has or appears to have control – this includes desks, lockers and bags.

A student's / pupil's possessions can only be searched in the presence of the student / pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the academy rules regardless of whether the rules say an item can be searched for.

## Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the academy rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the academy open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of academy discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The academy should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The academy may wish to add further detail about these arrangements.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main Academy Template Policies document. Local authorities / LSCBs may also have further guidance, specific to their area.

## Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the academy rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of academy discipline) or whether the material is of such seriousness that it requires the involvement of the police. (It is recommended that members of staff should know who to contact, within academy, for further guidance before taking action and that the person or persons is or are named within this policy).

A record should be kept of the reasons for the deletion of data / files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the academy can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the academy to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

## Care of Confiscated Devices

Academy staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices.

The academy in no way takes responsibility for pupils/ staff devices when they are in school.

## Audit / Monitoring / Reporting / Review

The responsible person (Headteacher) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the Online Safety Governor at regular intervals, on request.

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

DfE guidance can be found at: https://www.gov.uk/government/publications/searching-screening-and-confiscation

# Mobile Technologies Template Policy (inc. BYOD/BYOT)

Mobile technology devices may be a academy owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the academy's wireless network. The device then has access to the wider internet which may include the academy's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils / students, staff and wider academy community understand that the primary purpose of having their personal device at academy is educational and that this is irrespective of whether the device is academy owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

## Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, academys not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

For further reading, please refer to "Bring your own device: a guide for academys" by Alberta Education available at: http://education.alberta.ca/admin/technology/research.aspx and to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/bring-your-own-device-byod/

### Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your academy network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Academys may consider implementing the use of mobile technologies as a means of reducing expenditure on academy provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole academy community – including teachers - and the only effective way for a academy to implement these successfully is to involve the whole academy community from the outset. Before the academy embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

A range of mobile technology implementations is possible. Academy should consider the following statements and remove those that do not apply to their planned implementation approach.

- The academy Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies

| | Academy Devices | | | Personal Devices | | |
|---|---|---|---|---|---|---|
| | Academy owned and allocated to a single user | Academy owned for use by multiple users | Authorised device[3] | Pupil/Student owned | Staff owned | Visitor owned |
| Allowed in academy | **Yes** | **Yes** | **Yes** | Yes / No[4] | Yes / No[4] | Yes / No[4] |
| Full network access | Yes | Yes | Yes | | | |
| Internet only | | | | | | |

[3] Authorised device – purchased by the pupil/family through a academy-organised scheme. This device may be given full access to the network as if it were owned by the academy

[4] The academy should add below any specific requirements about the use of personal devices in academy, e.g. storing in a secure location, use during the academy day, liability, taking images etc

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| No network access |  |  |  |  |  |  |

- The academy has provided technical solutions for the safe use of mobile technology for academy devices/personal devices (delete / amend as appropriate):
  - All academy devices are controlled though the use of Mobile Device Management software
  - Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
  - The academy has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
  - For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
  - Appropriate exit processes are implemented for devices no longer used at a academy location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling academy-licenced software etc.
  - All academy devices are subject to routine monitoring
  - Pro-active monitoring has been implemented to monitor activity
- When personal devices are permitted:
  - All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
  - Personal devices are brought into the academy entirely at the risk of the owner and the decision to bring the device in to the academy lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in academy
  - The academy accepts no responsibility or liability in respect of lost, stolen or damaged devices while at academy or on activities organised or undertaken by the academy (the academy recommends insurance is purchased to cover that device whilst out of the home)

  - The academy accepts no responsibility for any malfunction of a device due to changes made to the device while on the academy network or whilst resolving any connectivity issues
  - The academy recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the academy. Pass-codes or PINs should be set on personal devices to aid security
  - The academy is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;
  - Devices may not be used in tests or exams
  - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
  - Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in academy
  - Personal devices should be charged before being brought to academy as the charging of personal devices is not permitted during the academy day
  - Devices must be in silent mode on the academy site and on academy buses
  - Academy devices are provided to support learning. It is expected that pupils/students will bring devices to academy as required.
  - Confiscation and searching (England) - the academy has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
  - The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
  - The software / apps originally installed by the academy must remain on the academy owned device in usable condition and be easily accessible at all times. From time to time the academy may add software applications for use

in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps

- The academy will ensure that academy devices contain the necessary apps for academy work. Apps added by the academy will remain the property of the academy and will not be accessible to students on authorised devices once they leave the academy roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- Printing from personal devices will not be possible

# Social Media Template Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The academy recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the academy, its staff, parents, carers and children.

## Scope

This policy is subject to the academy's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the academy.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the academy

The academy respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the academy's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a academy account or using the academy name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the academy are outside the scope of this policy.

Digital communications with pupils/students are also considered. Staff may use social media to communicate with learners via a academy social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

# Organisational control

## Roles & Responsibilities

- SLT
    - Facilitating training and guidance on Social Media use.

    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for Social Media accounts
    - Approve account creation
- Administrator / Moderator
    - Create the account following SLT approval
    - Store account details, including passwords securely
    - Be involved in monitoring and contributing to the account
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- Staff
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via academy accounts
    - Adding an appropriate disclaimer to personal accounts when naming the academy

## Process for creating new accounts

The academy community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the academy" Facebook page. Anyone wishing to create such an account must present a business case to the Academy Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the academy, including volunteers or parents.

## Monitoring

Academy accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a academy social media account.

## Behaviour

- The academy requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. Academy social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the academy.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to academy activity.
- If a journalist makes contact about posts made using social media staff must follow the academy media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the academy and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with academy policies. The academy permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The academy will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the academy will deal with the matter internally. Where conduct is considered illegal, the academy will report the

matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

## Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

## Handling abuse

- When acting on behalf of the academy, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, academy users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed academy protocols.

## Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

## Use of images

Academy use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the academy's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.

- Under no circumstances should staff share or upload student pictures online other than via academy owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on academy social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any academy list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

## Personal use

- Staff
  - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.
  - Personal communications which do not refer to or impact upon the academy are outside the scope of this policy.
  - Where excessive personal use of social media in academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
  - The academy permits reasonable and appropriate access to private social media sites.
- Pupil/Students
  - Staff are not permitted to follow or engage with current or prior pupils/students of the academy on any personal social media network account.
  - The academy's education programme should enable the pupils/students to be safe and responsible users of social media.
  - Pupils/students are encouraged to comment or post appropriately about the academy. Any offensive or inappropriate comments will be resolved by the use of the academy's behaviour policy
- Parents/Carers

- If parents/carers have access to a academy learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The academy has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the academy. In the event of any offensive or inappropriate comments being made, the academy will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the academy's complaints procedures.

### Monitoring posts about the academy

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the academy.
- The academy should effectively respond to social media comments made by others according to a defined policy or process.

# Appendix

### Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the academy logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

### Managing academy social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the academy
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the academy's reporting process
- Consider turning off tagging people in images where possible

### The Don'ts

- Don't make comments, post content or link to materials that will bring the academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of academy accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

## Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.

# Academy Policy Template – Online Safety Group Terms of Reference

## 1. Purpose

To provide a consultative group that has wide representation from the [academy/ academy] community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

### 2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group could include

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent / Carer
- ICT Technical Support staff (where possible)
- Student / pupil representation – for advice and feedback. Student / pupil voice is essential in the make-up of the online safety group, but students / pupils would only be expected to take part in committee meetings where deemed relevant.

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

## 3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

## 4. Duration of Meetings

Meetings shall be held regularly. A special or extraordinary meeting may be called when and if deemed necessary.

## 5. Functions

These are to assist the Online Safety Co-ordinator (or other relevant person) with the following

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole academy community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through[add/delete as relevant]:
- Staff meetings
- Student / pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for students / pupils, parents / carers and staff
- Parents evenings

- Website/VLE/Newsletters
- Online safety events
- Internet Safety Day (annually held on the second Tuesday in  February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the academy
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the [academy]
- To monitor incidents involving cyberbullying for staff and pupils

## 6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference have been agreed

Signed by (SLT): ---------------------------------------------------------------------

Date: ---------------------------------------------------------------------

Date for review: ---------------------------------------------------------------------

# Legislation

Academys should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

## Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

## Data Protection Act 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

## Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

## Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

## Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

## Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The academy reserves the right to monitor its systems and communications in line with its rights under this act.

## Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

### Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

### Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

### Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

### Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

## Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

## Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

## Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

## Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

## Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the academy context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion

- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The academy is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

## The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

## The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see DfE guidance - http://www.education.gov.uk/academys/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

## The Protection of Freedoms Act 2012

Requires academys to seek permission from a parent / carer to use Biometric systems

## The Academy Information Regulations 2012

Requires academys to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-academys-must-publish-online

## Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

# Links to other organisations or documents

The following links may help those who are developing or reviewing a academy online safety policy:

## UK Safer Internet Centre

Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

## CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

## Others

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

## Tools for Academys

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

## Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_Academy_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - http://www.childnet.com/new-for-academys/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

## Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

## Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

## Mobile Devices / BYOD

Cloudlearn Report Effective practice for academys moving to end locking and blocking

NEN - Guidance Note - BYOD

## Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Academys - ICO

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for academys (England)

ICO - Guidance we gave to academys - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in academys

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Academys on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting Academy Data

## Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

## Infrastructure / Technical Support

Somerset - Questions for Technical Support

NEN - Guidance Note - esecurity

## Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum

Online Safety BOOST Presentations - parent's presentation

Connectsafely Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

## Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Ofcom – Children & Parents – media use and attitudes report - 2015

# Glossary of Terms

| | |
|---|---|
| AUP / AUA | Acceptable Use Policy / Agreement – see templates earlier in this document |
| CEOP | Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes. |
| CPD | Continuous Professional Development |
| FOSI | Family Online Safety Institute |
| ES | Education Scotland |
| HWB | Health and Wellbeing |
| ICO | Information Commissioners Office |
| ICT | Information and Communications Technology |
| ICTMark | Quality standard for academys provided by NAACE |
| INSET | In Service Education and Training |
| IP address | The label that identifies each computer to other computers using the IP (internet protocol) |
| ISP | Internet Service Provider |
| ISPA | Internet Service Providers' Association |
| IWF | Internet Watch Foundation |
| LA | Local Authority |
| LAN | Local Area Network |
| MIS | Management Information System |

NEN National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to academys across Britain.

Ofcom Office of Communications (Independent communications sector regulator)

SWGfL South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for academys and other organisations in the SW

TUK Think U Know – educational online safety programmes for academys, young people and parents.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in April 2016. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with academy conduct or discipline.