Devonshire Primary Academy Online Safety Policy

Adopted by Governors/HT: Governors
Implementation date: May 2023
Review period: Annually
Last review date: May 2024
Person responsible for policy: Computing Lead & IT Technician

Intent

At Devonshire Academy, we believe that Online Safety is an integral part of children's education in today's digital world and should be embedded in their learning at school.

We also want to help our parents and children improve their own understanding of Online Safety issues so they can learn to use the internet and all digital media in a safe and secure way.

It is our intention that our pupils are well equipped with an Online Safety curriculum that is purposeful and provides pupils with the necessary knowledge and skills to keep themselves safe whilst using technology. To deliver our curriculum, we follow the National Curriculum and use Project Evolve as a planning tool for lesson delivery. This is part of the Computing spiral curriculum that ensures that Online Safety is taught as a prerequisite and then woven in line with our broad and balanced curriculum, in order to have optimum impact. Online Safety coverage is carefully planned within the Computing/Online Safety curriculum as taught in school.

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Headteacher
- Computing Lead
- Staff – including Teachers, Support Staff, Technical Staff
- Governors
- Parents and Carers

Schedule for Development / Monitoring / Review

The implementation of this Online Safety policy will be monitored by:	*Mr D Simm (Headteacher)* *Mr J Dodding (Computing Lead)* *Mr I Rawat (IT Technician)* *Mr D O'Brien (Chair of Governors)*
Monitoring will take place 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:	*May 2025*
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	*Police*

Scope of the Policy

This policy applies to all members of the academy community (including staff, pupils, volunteers, placement students, supply agency staff, contractors, parents / carers, visitors and community users) who have access to and are users of academy computing 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 / pupils 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. 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

- Approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher 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 Computing Lead.
- The Headteacher and (at least) another member of the Senior Leadership 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.
- The Headteacher is responsible for ensuring that the Computing Lead 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 will ensure that there is a system in place to allow for monitoring and support of those in the 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 Computing Lead.

Computing Lead

The Computing Lead:

- 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.
- Reports regularly to Senior Leadership Team.

IT Technician

The Technician, in collaboration with Blackpool Council IT Services 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 / 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 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 in order to effectively carry out their Online Safety role and to inform and update others as relevant
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Computing Lead for investigation.
- That monitoring software / systems are implemented and updated as agreed in academy policies.

Teaching and Support Staff

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 Acceptable Use Policy / Agreement.
- They report any suspected misuse or problem to the Headteacher / Computing Lead 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.
- Pupils understand and follow the Online Safety and acceptable use policies.
- 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 with regard to these devices.
- In lessons where internet use is pre-planned 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.

When using the Internet supervision is essential.

Designated Safeguarding Lead (DSL)

The DSL 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

Pupils

- Are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Policy.
- 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 the academy, if related to their membership of the academy.

Parents / Carers

Parents and 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, social media and information about national / local Online Safety campaigns and literature.

Community Users

Community Users who access academy systems as part of the wider academy provision will be expected to sign the Acceptable Use Policy / Agreement before being provided with access to academy systems.

Online Safety Curriculum

Online Safety is taught from EYFS to Year 6 in a planned and progressive way, ensuring all children are aware of their responsibilities in ensuring their safety and the safety of others. Online Safety is taught in a coherent way building on prior learning and to meet the needs of our children.

Lessons are monitored and pupil conferencing is used to ensure delivery is comprehensive. This is achieved through the Teach Computing curriculum and Evolve's excellent Online Safety resources.

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 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 curriculum once per half term. This has a specific focus and is outlined in the Computing Knowledge Organisers. The Online Safety resources and guidance is gathered from Project Evolve.
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / 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 helped to understand the need for the 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 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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 online 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
- Newsletters and social media
- Parents evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers, www.thinkuknow.com, www.ceop.police.uk

Education – The Wider Community

Where possible, the academy will provide opportunities for local community groups / members of the community to gain from the 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.
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision.

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:

- All new staff should receive the Online Safety policy and Acceptable Use agreements.
- The Computing Lead (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 Computing Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

Education & Training – Technical (infrastructure / equipment, filtering and monitoring)

The IT Technician, in collaboration with Blackpool Council IT Services, 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.
- All users will be provided with a username and initial password by the IT Technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. The IT Technician can reset passwords if required / requested.
- The “master / administrator” passwords for the academy ICT system, used by the IT Technician must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. academy safe).
- The IT Technician 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 to deal with requests for filtering changes.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the academy systems and data. These are tested regularly. 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. This will be through the staff acceptable usage policy or community acceptable usage policy.
- 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 that allows staff to / forbids staff from downloading executable files and installing programmes on academy devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on academy devices. Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.

Communications and Devices

Staff are provided with all the equipment that they need to teach effectively. Devices from home are not permitted. Pupils will also be provided with all the hardware that they need and therefore phones, tablets and other mobile devices are not to be used on the academy’s network.

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 pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying 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. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Visitors are not permitted to use their mobile phone on site. However, Senior Management may allow parents / carers to take a digital image of their own children at academy events on the understanding that it is for their own personal use. 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.
- 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 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the academy website.

Communication Devices	Staff & other: Allowed	Staff & other: Allowed at certain times	Staff & other: Allowed for selected staff	Staff & other: Not allowed	Pupils: Allowed	Pupils: Allowed at certain times	Pupils: Allowed with staff permission	Pupils: Not allowed
Mobile phones may be brought to academy	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on personal 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 (iMessage)	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 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 pupils or parents / carers (email, text, blog 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.
- 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 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 minimise risk of harm to pupils, staff and the academy through limiting access to personal information:

- Training to include: acceptable use; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.

Academy staff should ensure that:

- No full name reference should be made on the academy's social media to 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 / Trust or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The academy's use of social media for professional purposes will be checked regularly by the Computing Lead to ensure compliance with the Data Protection policy.

Unsuitable / Inappropriate 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 academy or outside academy when using academy equipment or systems. The academy policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using academy systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
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	

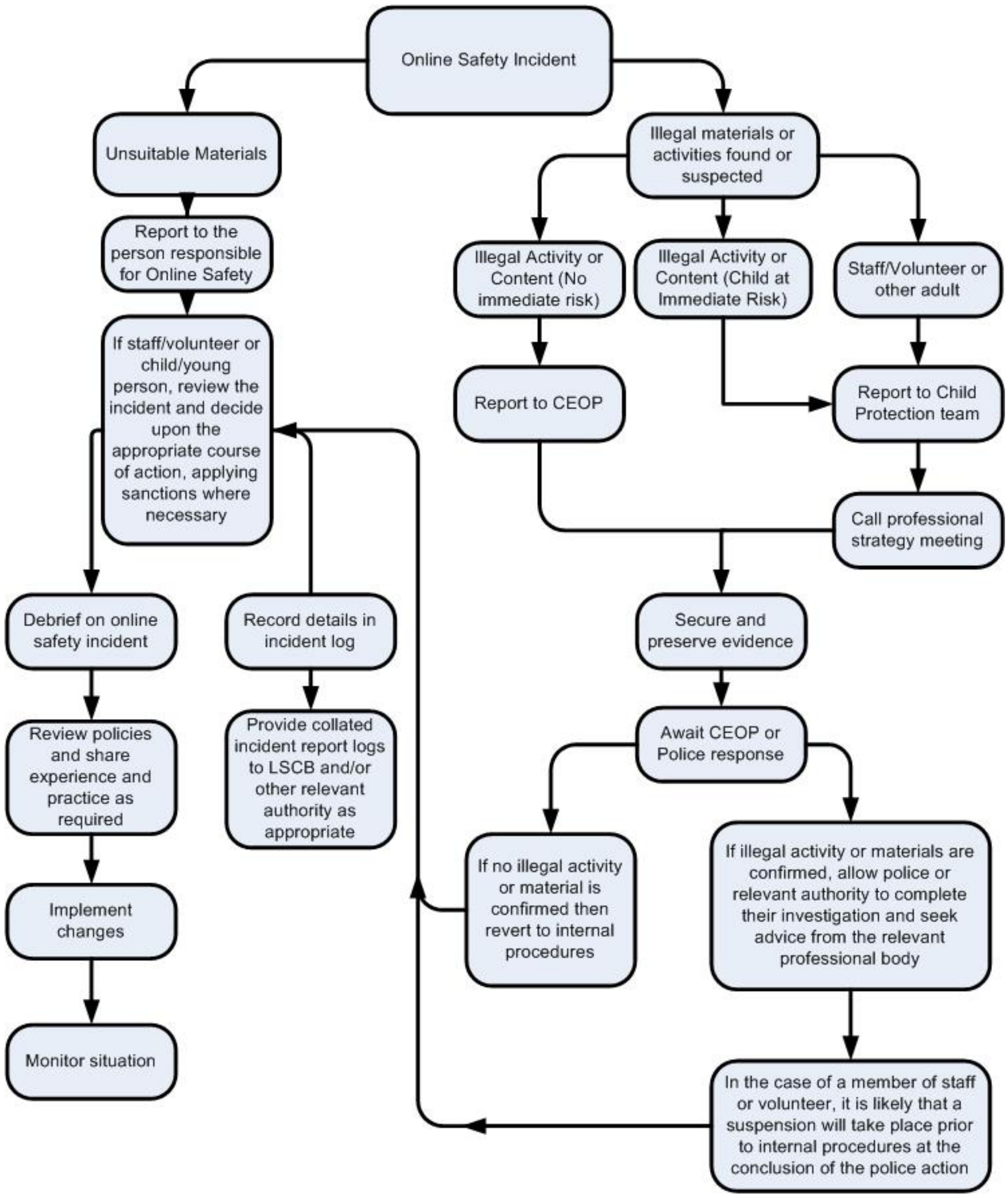
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube		X			

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" on the previous page).

Illegal Incidents

If there is any suspicion that the website(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 for responding to Online Safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow the 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 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 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
    - 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 of 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 child protection 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:

Students / Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Computing Lead	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. detention / 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
Unauthorised use of non-educational sites during lessons	X	X				X		X	X
Unauthorised use of mobile phone / digital camera / other mobile device	X	X				X			
Unauthorised use of social media / messaging apps / personal email	X	X				X			
Unauthorised downloading or uploading of files	X				X	X			
Allowing others to access academy / academy network by sharing username and passwords	X	X				X	X		
Attempting to access or accessing the academy / academy network, using another pupil's account	X	X				X		X	
Attempting to access or accessing the academy / academy network, using the account of a member of staff	X	X	X		X	X	X	X	
Corrupting or destroying the data of other users	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		
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X	X			X	X		X
Using proxy sites or other means to subvert the academy's / 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

Deliberately accessing or trying to access offensive or pornographic material	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

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / 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	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		
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		
Careless use of personal data e.g. holding or transferring data in an insecure manner	x				x			
Deliberate actions to breach data protection or network security rules	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	
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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	x	x	X	X	x		x	X
Actions which could compromise the staff member's professional standing	x	x		x	x	x	x	X
Actions which could bring the academy / academy into disrepute or breach the	x	x				x	x	X

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

Appendices

Legislation

Academies 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.

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 Harassment 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 I mages of children in the United Kingdom. A child for these purposes is 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

The new 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 template policy in these appendices and for DfE guidance - http://www.education.gov.uk/academys/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012

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

The Academy Information Regulations 2012

Requires academies to publish certain information on its website:
http://www.education.gov.uk/academys/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoacademyinformationregulations

Links to Other Organisations or Documents

- Safer Internet Centre -
- South West Grid for Learning
- Childnet
- Professionals Online Safety Helpline
- Internet Watch Foundation
- CEOP - http://ceop.police.uk/
- ThinkUKnow
- 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/index.aspx
- SWGfL BOOST

Cyberbullying

- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government Better relationships, better learning, better behaviour
- DCSF - Cyberbullying guidance
- DfE – Preventing & Tackling Bullying – Advice to academy leaders, staff and Governing Bodies
- Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

- Digizen – Social Networking
- 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
- Teach Computing – https://teachcomputing.org/
- Project Evolve - https://projectevolve.co.uk/
- Insafe - Education Resources

Mobile Devices / BYOD

- Cloudlearn Report Effective practice for academys moving to end locking and blocking
- NEN - Guidance Note - BYOD

Data Protection

- Your rights to your information – Resources for Academys - ICO
- ICO pages for young people
- 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 – Access Aware Toolkit
- 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
- Kent - Safer Practice with Technology
- 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 / Common Sense Media Digital Literacy & Citizenship Curriculum
- SWGfL BOOST Presentations - parents presentation
- Connect Safely - a Parents Guide to Facebook
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- DirectGov - Internet Safety for parents
- 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 - it’s not chalk and talk anymore!"

Glossary of Terms

AUP	Acceptable Use Policy – 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.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
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

Apps/Websites Reported by Parents

Parents can report via the school office, email (admin@devonshire.blackpool.sch.uk), directly to Mr Dodding or any member of school staff. Staff are obliged to pass the information on as soon as possible to the Computing Lead who will action according to the Online Safety policy.

Computing Long Term Plan

Devonshire Computing Long Term Plan

Year 1	Autumn	Spring	Summer
1st Half Term	Technology Around Us	Moving a Robot **BeeBots**	Digital Writing
Last Week	Privacy and Security + Managing Info	Online Relationships + Online Reputations	Health, Wellbeing and Lifestyles
2nd Half Term	Digital Painting	Grouping Data	Programming Animation
Last Week	Online Bullying	Self-Image and identity	Copyright and Ownership

Years 2	Autumn	Spring	Summer
1st Half Term	I.T Around Us	Pictograms	Digital Music
Last Week	Privacy and Security + Managing Info	Online Relationships + Online Reputations	Health, Wellbeing and Lifestyles
2nd Half Term	Digital Photography	Robot Algorithms **BeeBots**	Programming Quizzes
Last Week	Online Bullying	Self-Image and identity	Copyright and Ownership

Years 3	Autumn	Spring	Summer
1st Half Term	Connecting Computers	Sequences Sounds	Desktop Publishing
Last Week	Privacy and Security + Managing Info	Online Relationships + Online Reputations	Health, Wellbeing and Lifestyles
2nd Half Term	Stop Frame Animation	Branching Databases	Events and Actions
Last Week	Online Bullying	Self-Image and identity	Copyright and Ownership

Programming
Creating Media
Computer Systems
Data and Information

Devonshire Computing Long Term Plan

Year 4	Autumn	Spring	Summer
1st Half Term	The Internet	Repetition in Shapes	Photo Editing
Last Week	Privacy and Security + Managing Info	Online Relationships + Online Reputations	Health, Wellbeing and Lifestyles
2nd Half Term	Audio Production	Data Logging	Repetition in Games
Last Week	Online Bullying	Self-Image and identity	Copyright and Ownership

Years 5	Autumn	Spring	Summer
1st Half Term	Systems and Searching	Physical Computing: **Crumbles**	Vector Graphics
Last Week	Privacy and Security + Managing Info	Online Relationships + Online Reputations	Health, Wellbeing and Lifestyles
2nd Half Term	Video Production	Flat File Databases	Selection in Quizzes
Last Week	Online Bullying	Self-Image and identity	Copyright and Ownership

Years 6	Autumn	Spring	Summer
1st Half Term	Communication + Collaboration	Variables in Games	3D Modelling
Last Week	Privacy and Security + Managing Info	Online Relationships +Online Reputations	Health, Wellbeing and Lifestyles
2nd Half Term	Web Page Creation	Introduction to Spreadsheets	Sensing Movement: **MicroBits**
Last Week	Online Bullying	Self-Image and identity	Copyright and Ownership

Programming
Creating Media
Computer Systems
Data and Information