

Devonshire Infant & Junior Academies

Online Safety Policy

Scope of the Policy

This policy applies to all members of the academy community (including staff, pupils, volunteers, parents /carers, visitors, community users) who have access to and are users of academy digital technology 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 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 online-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 school.

Writing and Reviewing the Online Safety Policy

The implementation of this Online Safety policy will be monitored by the:	<i>Computing Lead and Senior Leadership Team</i>
Monitoring will take place at regular intervals:	<i>Annually</i>
The Governing Body 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:	<i>Annually</i>
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:	<i>March 2024</i>
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<i>Please see flowchart for responding to Online Safety incidents</i>

Roles and Responsibilities

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

The responsible member of the Senior Leadership Team is	<i>Elise Waldron</i>
The responsible member of the Academy Councillors is	<i>Harpal Tiwana</i>
The Designated Safeguard Lead is	<i>Pal Chahal</i>
The Online Safety lead in school is	<i>Pal Chahal/Olivia Waldron</i>

Policy Statements

Education – Pupils

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.
- 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, pupils should be guided to sites that are suitable for their use. If unsuitable material is found, this is reported to the Online Safety Lead for action.
- 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

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

- Curriculum activities
- Letters, newsletters, web site
- Parents/Carers evenings/designated sessions
- High profile campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk) www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

Education – Remote Education

We recognise the additional risks to pupils associated with being online more than before the pandemic. We also recognise additional risks for staff, especially those facilitating remote learning via video links that may impact other people in their household or community as well.

Online education should follow the same principles set out in our staff code of conduct which has been updated to reflect expected good remote education practice.

In addition to the updated codes of conduct, staff, pupils (or due to their age and ability, the adults supporting them), parents, carers, and to some degree, virtual or in-person visitors using online technology for education purposes or school business are expected to (with examples of support):

Security and Privacy

- Adjust privacy and safety settings on all devices, in apps and other online places to control what personal data is shared.
- Think about physical privacy when appearing live online e.g. the appropriate adult supervision of children at home, appropriate clothing, distractions like noise and interruptions, what other people nearby can hear.
- Never give out personal information to websites or in response to emails/text messages not recognised or trusted
- Follow the guidance given to all staff for holding Zoom meetings with children.

Stay physically and mentally healthy online

- Whether staff or pupils are working, learning or playing online, they should take regular breaks
- Parents and carers will be given guidance on supporting their child's mental health and wellbeing during COVID-19. School will participate in event such as Children's Mental Health Awareness week and screen free days.

Keep talking about staying safe online

- Signpost parents and carers to tools to explain and reduce risks, and help them talk to their child.
- Engage in activities for internet safety and Internet Safety Day reminding children how to stay safe.
- Staff should pay special attention to how they protect personal data at home.
- Staff should engage in regular or update PREVENT training.

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 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 Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Technical – infrastructure/equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements.
- 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 secure password. Users are responsible for the security of their username and password and will be required to change their password every 2 months.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are updated and internet use is logged and monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The academy has provided differentiated user-level filtering
- Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. This is achieved through the use of Entrust filtering software.
- Users can report a breach of security to the appropriate staff member of the following: Headteacher, Senior Leader or Online Safety Lead.
- 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 school systems and data. The school 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" (eg trainee teachers, supply teachers, visitors) onto the school systems. Upon completing their school induction, they will agree to use the academy's network responsibly, as set out in the Staff Acceptable Use Policy.
- Staff are unable to install executable files on the academy network. If staff need to install a program, they will ask the Network Manager, who will check the file appropriately, then install it according to our network guidelines.
- Staff agree to not use removable media on academy devices (e.g. memory sticks). Appropriate DVDs and CDs that have been purchased by the academy may be used. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage.

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

The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	No	No	No	No	No	No
No network access	No	No	No	Yes	Yes	Yes

Use of digital and video images

Staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press
- 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 is 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 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 photograph
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Communications

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

Communication Technologies	Staff & other adults				Students / Pupils			
	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	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices	✓					✓		
Use of personal email addresses in academy , or on academy network				✓				✓
Use of academy email for personal emails				✓				✓
Use of messaging apps			✓					✓
Use of social media	✓							✓
Use of blogs	✓							✓

Social Media - Protecting Professional Identity

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school 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 unless it is done so within a professional manner, with a view to support the CPD of other academy teachers
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the academy or MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- 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 school are outside the scope of this policy
- The academy permits reasonable and appropriate access to private social media sites

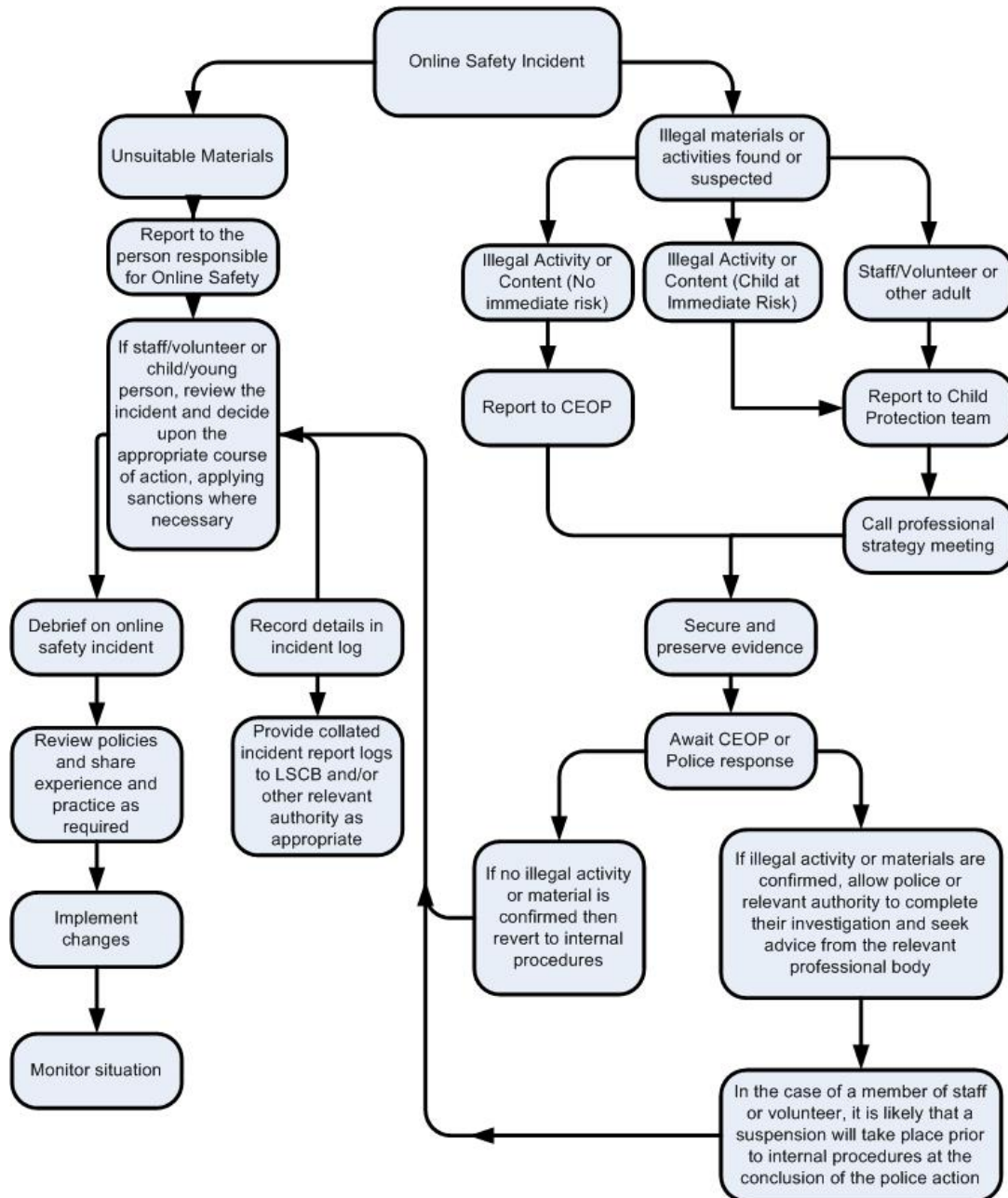
Dealing with unsuitable/inappropriate activities

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/or outside the 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	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (eg 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			

Illegal Incidents Flowchart

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) for responding to online safety incidents and report immediately to the police.



Appendix:

Legislation

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 1998

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 school 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 images 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

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, connections 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 school 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 school 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 school 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.

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

The Protection of Freedoms Act 2012

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

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-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 school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning – <https://swgfl.org.uk/products-services/online-safety/>

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

[LGfL – Online Safety Resources](#)

[Kent – Online Safety Resources page](#)

INSAFE / Better Internet for Kids – <https://www.betterinternetforkids.eu/>

UK Council for Child Internet Safety (UKCCIS) – www.education.gov.uk/ukccis

Netsmartz - <http://www.netsmartz.org/>

Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self review tool: www.360data.org.uk

Bullying / Online-bullying / Sexting / Sexual Harrassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

[Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm](http://www.antibullying.net/cyberbullying1.htm)

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

Data Protection

[360data - free questionnaire and data protection self review tool](#)

[ICO Guide for Organisations \(general information about Data Protection\)](#)

[ICO Guides for Education \(wide range of sector specific guides\)](#)

[DfE advice on Cloud software services and the Data Protection Act](#)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Computing](#)

[ICO - Guidance we gave to schools - September 2012](#)

[IRMS - Records Management Toolkit for Schools](#)

[NHS - Caldicott Principles \(information that must be released\)](#)

[ICO Guidance on taking photos in schools](#)

[Dotkumo - Best practice guide to using photos](#)