THE WHITCHURCH CHURCH OF ENGLAND FEDERATION

E-Safety Policy
Implementation Date – June 2020
Review Date – June 2021

CONTENTS

Appendices

E-Safety Policy

1. Introduction

E-safety is often defined as the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (e.g. text messages, email, gaming devices etc.).

E-safety is not just about technology, it is also about people and their actions.

Technology provides unprecedented access to new educational opportunities; online collaboration, learning and communication. At the same time, it can provide the potential for staff and pupils to access material they shouldn't, or be treated by others inappropriately.

E-safety is part of the wider duty of care of all those who work in schools: equipping children and young people to stay safe online, both in school and outside, is integral to a school's Computing curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and Sex and Relationship Education (SRE) and include how students should report incidents (e.g. The Child Exploitation and Online Protection (CEOP) button, via a trusted adult, Childline etc.)

General advice and resources for schools on internet safety are available at:
https://www.saferinternet.org.uk/

In association with the St Bart's Multi-Academy Trust Acceptable Use Policy (AUP), this policy forms part of the Federation's commitment to educate and protect all users when accessing digital technologies, both within and outside the academies. It should be read in conjunction with other relevant policies, such as the Child Protection/ Safeguarding, Behaviour and Anti-Bullying policies.

In England, schools are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. Since 2015 there have been additional duties under the Counter Terrorism and Security Act 2015, known as the 'Prevent duty', which require schools to ensure that children are safe from terrorist and extremist material on the internet, to prevent people from being drawn into terrorism.

Ofsted judges as 'outstanding', schools where '*students have an excellent understanding of how to stay safe online and of the dangers of inappropriate use of mobile technology and social networking sites*'.

(Source: Ofsted School Inspection Handbook - October 2017)

This policy will be reviewed annually and/or more frequently in line with new developments in the use of the technologies, new threats to online safety or the level and/or nature of incidents reported.

2. Scope

This policy applies to all members of the Federation community, including staff, governors, pupils, volunteers, parents, carers, visitors and community users. This includes anyone who uses and/or has access to, personal devices and technologies whilst on any of our academy sites and those who have access to, and are users of, Federation devices and technologies, both in and outside of the school.

The Education and Inspections Act 2006 empowers Heads to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school / academy sites, 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 academies but is linked to membership of the academies.

The Head of School of each academy will, where it becomes known, inform parents/carers of any such incidents of inappropriate online behaviour that takes place out of the academy.

The 2011 Education Act increased these powers with regard to the searching for electronic devices and the examination of any files or data (even where deleted), on such devices. In the case of both acts, action will be taken in line with the Federation's published Behaviour Policy or St Bart's Disciplinary procedures.

The Federation will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date and reflect changes or amendments such as a member of staff who has left the Federation or a pupil whose access has been withdrawn.

3. The Prevent Duty

As organisations seek to influence young people through the use of social media and the internet, schools and childcare providers need to be aware of the increased risk of online radicalisation and the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty is the duty under the Counter-Terrorism and Security Act 2015 on specified authorities (schools and childcare providers), in the exercise of their functions, to have due regard for the need to prevent people from being drawn into terrorism. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are required to identify risks within a given local context and identify children who may be at risk of radicalisation, and know what to do to support them.

The Prevent duty requires school monitoring and filtering systems to be fit for purpose. The school has a filtering system in place and its effectiveness is continuously monitored by the Head of School.

The Prevent duty means that all staff have a duty to be vigilant, and where necessary, will report concerns about internet use that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

All staff should be aware of the following:

1. DfE Prevent duty
2. DfE briefing note on the use of social media to encourage travel to Syria and Iraq
3. The Channel Panel
4. Terrorism Act 2000 and the disclosure of information duty where it is believed or suspected that another person has committed an offence.

Practical advice and information for teachers, parents and school leaders on protecting children from extremism and radicalisation is available at:
https://www.educateagainsthate.com/

The Department for Education has dedicated a telephone helpline (020 7340 7264) to enable staff and governors to raise concerns relating to extremism directly. Concerns can also be raised by email to:
counter.extremism@education.gsi.gov.uk

Please note that the helpline is not intended for use in emergency situations, such as a child being at immediate risk of harm or a security incident, in which case the normal emergency procedures should be followed.

4. Governing Legislation

It is important to note that in general terms an action that is illegal if committed offline, is also illegal if committed online.

Computer Misuse Act 1990
Data Protection Act 1998
Freedom of Information Act 2000
Communications Act 2003
Malicious Communications Act 1988
Regulation of Investigatory Powers 2000
Copyright, Designs and Patents Act 1988
Telecommunications Act 1984
Criminal Justice & Public Order Act 1994
Racial and Religious Hatred Act 2006
Protection from Harassment Act 1997
Protection of Children Act 1978
Sexual Offences Act 2003
Public Order Act 1986
Obscene Publications Act 1959 and 1964
Human Rights Act 1998
The Education and Inspections Act 2006
The Education and Inspections Act 2011
The Protection of Freedoms Act 2012
The Schools Information Regulations 2012
Serious Crime Act 2015
Terrorism Act 2000
Further explanatory detail about governing legislation can be found in Appendix C.

5. Roles & Responsibilities

E-safety is seen as a 'whole school' issue, with specific responsibilities delegated as follows:

	Whitchurch CE Infant & Nursery Academy	**Whitchurch CE Junior Academy**
Head of School	Mrs Julie Rowlandson	Ms Sarah Walsh
Designated Safeguarding Lead(s)	Mrs Sarah Cope Mrs Julie Rowlandson	Mrs Sarah Cope Ms Sarah Walsh
Computing Subject Leader	Ms Cathie Hunter	Mr Nick Armstrong
Technician	Mr Kieron Viggars	Miss Natalie Williams

A full description of the responsibilities associated with these roles may be found in Appendix B.

6. Definitions: Devices & Technology

Device(s)	Examples include but are not limited to: • Personal computers • Laptops • Tablets

	- ‘Smart’/Mobile phones - ‘Smart’ watches - Cameras - USB sticks/flash drives
Technology(ies)	Examples include but are not limited to: - Internet search engines - Websites - Social media platforms, e.g. Facebook, Twitter, Instagram, Snapchat, WhatsApp, YouTube - Real time communications e.g. texts, chat rooms, email, instant messaging, Skype, FaceTime, video chat, Zoom, Teams - On-line gaming, e.g. Xbox, PlayStation

7. School Staff, Governors and Volunteers

Acceptable Use Policy Agreements

Before being granted access to any of the academy devices and technologies, all members of the Federation community (staff, Governors and Volunteers) are required to read St Bart’s Multi-Academy Trust Acceptable Use Policy Agreement (AUP).

Acceptable Use Policy (AUP) for Staff

All staff must read and sign the St Bart’s Multi-Academy Trust ‘Acceptable Use Policy (AUP) before using any of an academy’s IT resource.

A copy of the SBMAT staff AUP will be issued to all new members of staff during Induction. The individual academies will also issue the AUP to staff, periodically, in response to the nature and/or volume of reported incidents, changes in legislation and emerging trends in online behaviour.

Access to online services and an academy’s devices will not be approved until new staff have read and signed the AUP.

E-safety and the AUP are included in the statutory induction for all new staff and forms part of the contract of employment.

Acceptable Use of Devices and Technologies: Staff

Any device provided by either academy to or for staff or pupils, is primarily intended to support the teaching and learning of pupils. Discretion and the highest professional standards of conduct are expected of staff using academy devices for personal use.

Where remote access to the academy network via a personal device is approved by the Head of School, staff confirm their acceptance of the terms set out in the Acceptable Use Policy in relation to that device. Staff should seek clarification of any terms and conditions they do not understand.

Staff breaches of the AUP

Where a staff member is found to be in breach of the SBMAT AUP, the matter will be dealt with in accordance with appropriate Federation or Trust policies such as the Disciplinary procedure, and /or with reference to external agency guidance.

8. Pupils

Acceptable Use Policy (AUP) for Pupils

The AUP for pupils can be found in Appendix A.

A copy of the pupil AUP is sent to parents with a covering letter/reply slip, at the start of the academic year, and to new pupils when they enrol. Pupils will not be given online access or allowed to use any of the academy devices before the AUP has been signed and returned to the respective academy offices.

Pupil breaches of the AUP

Where a pupil is found to have breached the AUP, this will be dealt with appropriately and in line with appropriate policies, such as the Behaviour Policy.

9. Using non-School Equipment – 'Bring Your Own Device' (BYOD)

The Federation acknowledges that the use of ICT within the teaching and learning setting can have benefits for staff and pupils. In some circumstances, the use of personal devices within the classroom setting can enhance the range of resources available to the class. However, this must be done in a way that does not compromise the integrity of the academies' IT networks, or leave staff or pupils at the risk of being able to access inappropriate content. In order to facilitate teaching and learning, we allow the use of personal IT devices within the Federation environment, subject to some simple rules. The St Bart's Multi-Academy Trust Bring Your Own Device policy should be read in conjunction with this policy. Its content applies to the use of personal IT devices and resources within the classroom or office setting. It does not apply to staff use of smartphones or personal tablets or laptops while connected to the academy internet. This is governed by the Acceptable Use Policy.

10. Security and passwords

Passwords should be changed regularly and must not be shared. Staff must always 'lock' a device (e.g. a classroom PC) if they are going to leave it unattended.

NB. The picture 'mute' or picture 'freeze' option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'.

All users should be aware that the ICT system is filtered and monitored.

11. Data storage

Memory sticks are not secure and are easily mislaid. There are many preferable alternatives to using memory sticks to transfer and access documents away from the school site. This might include using the academy One Drive/Google Drive and academy email accounts for storing and accessing documents or data. If there is no alternative to using a memory stick, for example if you do not have internet access at your off-site workplace, then the memory stick must be encrypted and can only be used if express permission has been granted by the Head of School.

12. Mobile phones, cameras and other devices

St Bart's Multi-Academy Trust is very clear that personal devices should not be used to take images or videos of learners. This is in line with our safeguarding obligations, and protects learners, staff and the reputation of the Federation.

Academy issued cameras / smartphones / laptops are available for trips, activities or recordings of performances. If these are used, they should be returned to the appropriate academy office / IT department after use, to have the photographs or videos uploaded to academy storage areas and wiped from the IT device.

Staff will be made aware of any learners who have not given consent to have their photograph taken. Every care will be taken to ensure that they are not included in any group photographs or other images.

13. Social Media and Networking

The expectations around the use of social media are set out in the St Bart's Multi-Academy Trust AUP and Social Networking protocol.

14. Cyber bullying

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole Federation. Every school / academy must have measures in place to prevent all forms of bullying. These measures should be part of the anti-bullying policy which must be communicated to all pupils, staff, governors and parents.

Cyber bullying is defined as '*the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them*.'

Cyberbullying against staff

The DfE state that '*all employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by pupils, parents and other members of staff, and supporting them if it happens*'.

Cyberbullying: Advice for head teachers and school staff is non-statutory advice from the Department for Education for head teachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Please refer to Appendix F for further guidance and support in dealing with instances of cyberbullying against staff and/or pupils.

15. Staff Reporting of E-safety Incidents and Concerns

The Federation takes the reports of incidents and concerns extremely seriously. Any subsequent action or remedy to be taken following the investigation of an incident or concern, will depend on its nature, situational and circumstantial factors.

All incidents that come to the attention of Federation staff should be notified to the Designated Safeguarding Lead via the academy reporting mechanism set out in Appendix E, or, where applicable, via the St Bart's Multi-Academy Trust Whistleblowing Policy.

Any incident that raises child protection or wider safeguarding questions must also be communicated to the Designated Safeguarding Lead(s) immediately.

Incidents that are of a concern under the Prevent duty should be referred to the Designated Safeguarding Lead immediately.

16. Staff training and updates

All staff have E-safety training included as part of their safeguarding induction to the Federation and receive regular training in safeguarding students. E-safety is included as part of this.

17. Communicating the E-safety Policy

Staff and the E-safety policy

- All staff will be given a copy of the E-safety Policy during statutory induction and its importance explained.
- The SBMAT Acceptable Use Policy is read and signed before access to academy devices and systems is approved and the agreement forms part of the contract of employment.
- Staff are made aware that internet traffic can be monitored and traced to the individual user, including on personal devices where network access has been granted. Because of this, discretion and professional conduct are essential at all times.

Introducing the E-safety policy to pupils

- Pupils are made aware that network and Internet use is monitored.

Home-School Communication of E-safety information

- The Federation website provides information on E-safety and how the Federation can help to support and guide their child
- E-safety advice is included as a regular feature in newsletters and as part of the ongoing dialogue between home and school.
- The school holds E-safety events to brief parents and carers about E-safety developments and policies;

18. Shropshire Safeguarding Contact details:

Local Authority Designated Officer (LADO)	lado@shropshire.gov.uk
Emergency Duty Team	0345 678 9040 01743 249544 (Out of hours only)

19. Monitor & review

This policy will be monitored continuously. It will be reviewed annually, and/or more frequently in line with new developments in the use of the technologies, new threats to online safety or level and/or nature of incidents reported.

Appendix A - AUP

AUP for Pupils

I want to feel safe all the time.

I know that anything I do on the computer can be seen by other people.

I know when to use the CEOP report button CEOP REPORT ceop.police.uk

I agree that I will:

- not use my own mobile phone, or any other device, in the academy
- always keep my passwords safe and not share them with anyone
- only open web pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or unhappy on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel sad or worried
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home, my family or my pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Signed ______________________________ ***Date*** __________________________

Appendix B: E-safety Roles & Responsibilities: List of duties

Head of School of each academy	• Has overall responsibility for E-safety provision. • Has overall responsibility for data and data security • Ensures that the academy uses an appropriate filtered Internet Service • Ensures that staff receive appropriate training to enable them to carry out their E-safety roles • Can direct the whole academy community including staff, students and governors to information, policies and practice about E-safety. • Is aware of the procedures to be followed in the event of a serious E-safety incident. • Receives regular monitoring reports • Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures and reviews (e.g. IT technician). • Oversees the administration of the staff Acceptable Use Policy and takes appropriate action where staff are found to be in breach.
Designated Safeguarding Lead/ Computing Subject Leader of each academy	• Takes day to day responsibility for E-safety issues and assumes a leading role in establishing and reviewing the school E-safety policies and supporting documents. • Ensures that the academy is compliant with all statutory requirements in relation to the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the Data Protection Act 1998. • Promotes an awareness of and commitment to E-safety throughout the academy community. • Ensures that E-safety is embedded across the curriculum. • Is the main point of contact for pupils, staff, volunteers and parents who have E-safety concerns • Ensures that staff and pupils are regularly updated on E-safety issues and legislation, and are aware of the potential for serious

	child protection issues that arise from (for example): - sharing of personal data - access to illegal/inappropriate materials - inappropriate on-line contact with adults/strangers - cyber-bullying • Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident. • Ensures that an E-safety incident log is kept up to date through CPOMS. • Liaises with academy IT technical staff where necessary and/or appropriate. • Facilitates training and provides advice and guidance to all staff. • Communicates regularly with SLT to discuss current issues, review incident logs and filtering.
Computing Subject Leader of each academy	• Oversees the delivery of the E-safety element of the Computing curriculum. • Communicates regularly with the Head of School / Designated Safeguarding Lead

IT Technician of each academy	• Oversees the security of the academy ICT system. • Ensures that appropriate mechanisms are in place to detect misuse and malicious attack (e.g. firewalls and antivirus software) • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Ensures that the academy's web-filtering is applied and updated on a regular basis. • Ensures that access controls/encryption exist to protect personal and sensitive information held on academy-owned devices. • Ensures that users may only access the academy networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • Reports any E-safety incidents or concerns, to the Designated Safeguarding Lead / Head of School. • Keeps up to date with the academy's E-safety policy and technical information in order to carry out the E-safety role effectively and to inform and update others as relevant. • Keeps up-to-date documentation of the academy's E-security and technical procedures. • Keeps an up to date record of those granted access to academy systems.
ALL Staff of each academy	• Read, understand and help promote the Federation E-safety policies and guidance. • Are aware of E-safety issues relating to the use of any digital technology, monitor their use, and implement Federation / Trust policies with regard to devices. • Report any suspected misuse or problem to the Designated Safeguarding Lead / Head of School. • Maintain an awareness of current E-safety issues and guidance, e. g. through training and CPD. • Model safe, responsible and professional behaviours in their own use of technology. • Ensure that any digital communications with students are on a professional level and through academy-based systems ONLY. • Ensure that no communication with pupils, parents or carers is entered into through

	personal devices or social media. - Ensure that all data about pupils and families is handled and stored in line with the principles outlined in the SBMAT AUP.
Teaching Staff	- Embed E-safety issues in all aspects of the curriculum and other academy / Federation activities. - Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended academy activities, where relevant). - Ensure that pupils are fully aware of how to research safely online and of potential legal issues relating to electronic content such as copyright laws.
Pupils	- Are responsible for using the academy digital technology systems in accordance with the Pupil AUP Agreement. - Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
Parents / Carers	- Parents and carers are encouraged to support the academies in promoting good online safety practice and to follow guidelines on the appropriate use of: digital and video images taken at academy / Federation events.
External groups	Any external individual/organisation must sign the SBMAT Acceptable Use Policy prior to using any equipment or the Internet within any of the academy buildings.

Appendix C: Legislation - Overview of relevant legislation governing E-safety

Schools should be aware of the legislative framework under which this E-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 HR and/or legal advice is sought in the event of an E-safety incident 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 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 personal 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.

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, or that of others. 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 person having 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 to releasing it, a criminal offence.

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 Head teachers, 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 Head teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

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

Appendix D: Examples of potential E-safety concerns (Pupils)

The following are provided by way of guidance and are in no way limiting or exhaustive. You should seek advice from the Designated Safeguarding Lead / Head of School if you are unsure about what might constitute a concern.

Inappropriate material accessed on Federation computers

Due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer even when filtering is in place and users abide by the rules.

Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting and are encouraged to alert staff to any inappropriate content. The staff member should report the incident to the Designated Safeguarding Lead/ Head of School who will log the problem and liaise with the IT technician to make any necessary adjustment to filter settings.

Abusive messages on Federation computers

Students who receive abusive messages over academy / Federation systems will be supported, and advised not to delete messages. The Designated Safeguarding Lead / Head of School will be informed and a formal process of investigation initiated.

Parent/Carer/Guardian reports of cyber bullying

Parents, carers and guardians may become aware that their child is concerned or upset by bullying, originating in the Academy / Federation but continuing via electronic means. Parents and carers should know that the academies encourage them and/or pupils to approach them for help, either via a staff member or directly to the Head of School. Such incidents will be investigated and dealt with in accordance with the Federation Behaviour/Anti-Bullying policy.

Pupil disclosure of concerns or abuse

All staff receive Safeguarding and E-safety training as part of their induction, and thereafter on a regular basis. Where a pupil discloses a concern to a member of Federation staff, this is passed on to the Designated Safeguarding Lead / Head of School.

Pupil reporting outside school

Students are taught that if something worries them, or if they think a situation is getting out of hand, that they should share this with a trusted adult such as their parents, carers, guardians or Federation / Academy staff.

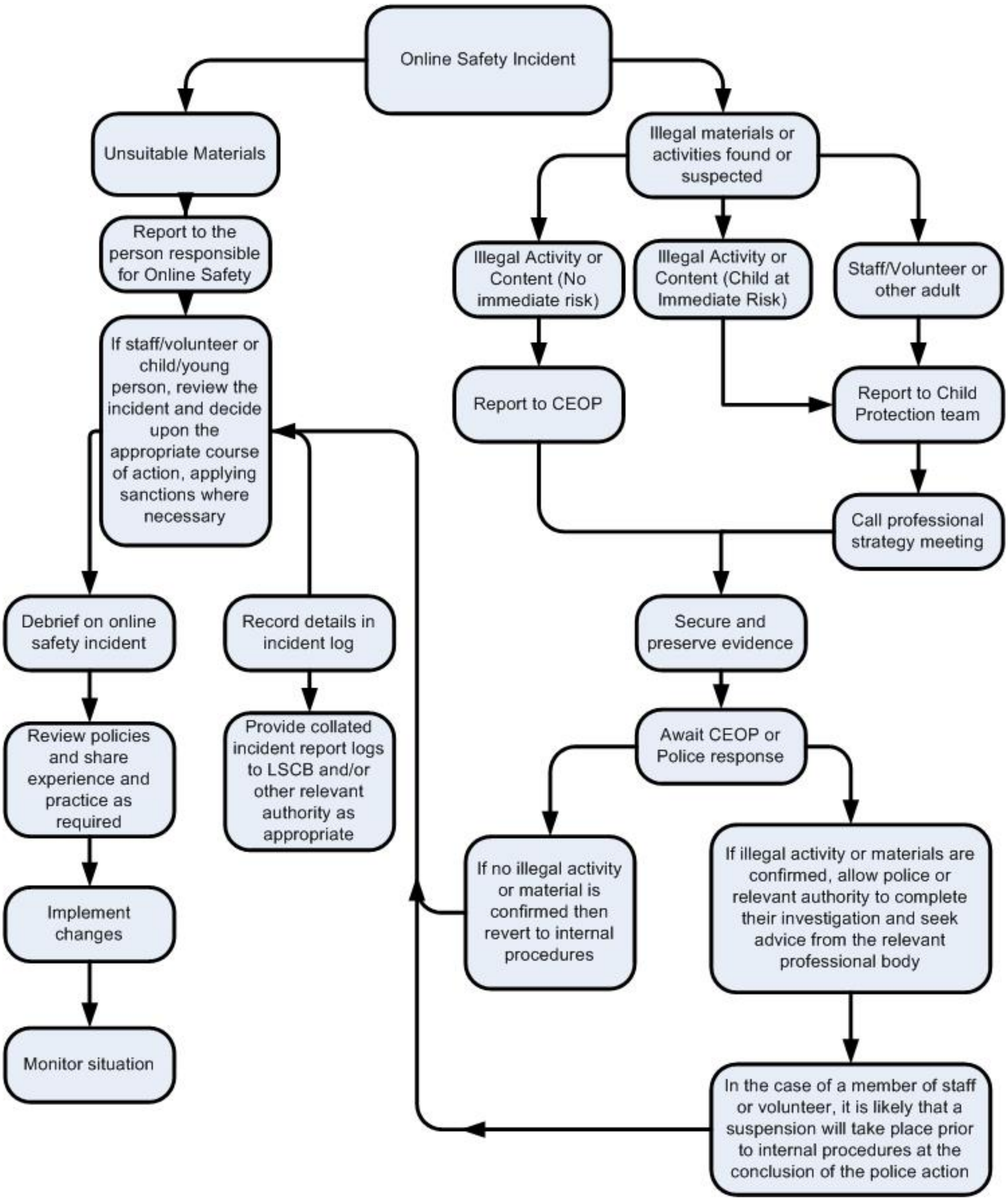
Allegations against staff

Allegations involving staff should ordinarily be reported to the Head of School or through the Whistleblowing Policy. If the allegation is one of abuse, then it should be handled in line with the statutory DfE guidance: 'Dealing with allegations of abuse against teachers and other staff'. If necessary local authority's LADO should be informed.

Evidence of incidents must be preserved and retained and where necessary, the LADO informed.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline)

Appendix E: Recording and 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

Appendix F: Cyberbullying: further advice and guidance

Behaviour that is classed as cyber bullying includes but is not limited to:

- **Abusive comments**, rumours, gossip and threats made over the internet or using digital communications – this includes internet trolling.

- **Sharing pictures**, videos or personal information without the consent of the owner and with the intent to cause harm and/or humiliation.

- **Hacking** into someone's email, phone or online profiles to extract and share personal information, or to send abusive or inappropriate content whilst posing as that person.

- **Creating specific websites or 'pages' on the Internet** that negatively target an individual or group, typically by posting content that intends to humiliate, ostracise and/or threaten.

- **Blackmail**, or pressurising someone to do something online they do not want to do such as sending a sexually explicit image.

Cyberbullying: Advice for head teachers and school staff

The Department for Education has produced non-statutory advice for head teachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

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

Preventing and tackling bullying: Advice for head teachers, staff and governing bodies

This document has been produced by the Department for Education to help schools take action to prevent and respond to bullying as part of their overall behaviour policy. It outlines, in one place, the Government's approach to bullying, legal obligations and the powers schools have to tackle bullying, and the principles which underpin the most effective anti-bullying strategies in schools. It also lists further resources through which school staff can access specialist information on the specific issues that they face. This includes cyberbullying.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf