Title	Online Safety
Associated Policies	• Safeguarding and Child Protection (TPO/HS/05) • Peer on peer abuse (TPO/HS/12) • Professional and Safe Conduct (TPO/STA/10) • Whistleblowing (TPO/STA/19) • Anti-Bullying (TPO/STU/01) • Student Care and Welfare (TPO/STU/06) • Data Protection (TPO/STA/25) • Behaviour and Discipline (TPO/STU/03) • Anti-Bullying (TPO/STU/01)

REVIEWED: September 2021 NEXT REVIEW: September 2022

Or as required in response to developments (e.g COVID-19 pandemic, local issues etc.)

1. Policy Statement

1.1 Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside the Trust's statutory Safeguarding and Child Protection Policy. Any issues and concerns with online safety must follow safeguarding and child protection procedures.

1.2 The Brooke Weston Trust is committed to promote the welfare and safety of our students when using digital technologies. The Trust recognises the importance of the contribution it can make to protecting and supporting students across its Academies in their use of these technologies.

1.3 This policy aims to:

- Set out expectations for all members of the community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).
- Incorporate all aspects of child protection and safeguarding that may be affected by digital technology as well as Brooke Weston Trust's use of technology with its Academies.
- Highlight the importance of online safety as a safeguarding issue.

- Outline how the Trust has responded to the COVID-19 pandemic and the subsequent demands for remote learning.

1.4 The Trust aims to have robust processes in place to ensure the online safety of students, staff, volunteers and governors. This will be achieved by establishing clear mechanisms to identify, intervene and escalate an incident where appropriate.

1.5 An effective approach to online safety, empowers us to protect and educate each Academy community in its use of technology.

1.6 The Trust will refer to the most recent government, DfE and ICO guidance and documentation with regard to Data Protection, data storage and privacy compliance.

2. How should this policy be applied?

2.1 This policy applies to all members of the Trust (all students, staff, governors, parents/carers and volunteers).

2.2 This policy applies to any individual who is given access to BWT's digitally connected systems (including email addresses and any other data source or system that is hosted/operated/controlled remotely or other by the Trust).

2.3 BWT expects all Academies will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding the use of technology and the Internet both on and off the school site. This will include imposing rewards and sanctions for behaviour – as defined as regulation or student behaviour under the Education and Inspections Act 2006. The 'In Loco Parentis' duty allows the academy to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

2.4 The Online Safety policy covers the use of:

- The Online safety curriculum intent, delivery and impact.
- School based IT systems.
- School based intranet and networking.
- School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, and social media websites.
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing.
- School IT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets
- Student and staff personal IT equipment when used in school and which makes use of school networking, file-serving or Internet facilities.
- Tablets, mobile phones, devices and laptops when used on the school site.

3. Who is responsible for carrying out this policy?

3.1 Principals should ensure that all academy staff and governors are aware of the Online Safety policy and procedure and of their responsibilities under it. It is the responsibility of the Principal to ensure that breaches of the policy are investigated and addressed.

3.2 Staff and governors are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place students or vulnerable adults at risk, bring the school into disrepute or damage their own professional reputation.

3.3 The implementation of this policy will monitored by the Academy's Senior Leadership Team and governors and remain under review by The Brooke Weston Trust (Safeguarding Review Group).

3.4 All staff, students, parents and carers have responsibilities as outlined in this policy. Online safety is everyone's responsibility.

4. What are the principles behind this policy?

4.1 Online safety risks are traditionally categorised as one of the **4 Cs: Content, Contact, Conduct** or **Commerce.**

These areas remain a helpful way to understand the risks and potential response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all four.

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and /or pornography, sharing other explicit images and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If staff, pupils or students feel at risk, please report it to the Anti-Phishing Working Group apwg.org

4.2 The most likely areas of risk to students are:

- Exposure to illegal inappropriate or harmful material
- Subject to harmful online interactions with other users
- The individuals' personal online risky behaviour that then leads to harm.

This is not exhaustive.

4.3 The definition of an online incident is:
"*Any incident that occurs and involves any person (student or adult) where the use of technology (equipment and/or networks) enables or facilitates inappropriate behaviour and harm and/or distress is caused to another person or the reputation of the Academy and/or BWT. This may include the use of social media, forums, blogs, open and closed groups, digital images, messages or any other means.*"

Examples of issues that may be part of an incident include:

- Youth produced imagery (sexting)
- Peer on peer abuse - cyber bullying
- Sexual abuse – 'grooming'
- Upskirting
- Sexual harassment
- CCE/CSE
- County Lines
- Radicalisation – extremism, radicalisation and terrorism
- Homophobic/transgender/racist/faith based/offensive language or behaviour
- Breaches of filtering
- Illegal content.

This is not an exhaustive list.

4.4 The Trust has a responsibility for ensuring that the resources are available to promote the safe use of technology and to promote understanding and awareness of the risks attached to the use of digital technology.

4.5 The Trust seeks to promote the use of technology and connectivity to ensure that the students are equipped with the necessary skills and knowledge to perform to the best of their ability both during their time in their Academy and also in their future in their chosen careers and workplaces.

4.6 Staff and students must be able to use digital technology appropriately and safely and understand the risks related to their activity. Students will receive online safety education as soon as they start using digital technology and will be continually reinforced and monitored as students' progress through their school life.

4.7 That Academy's use their reasonable endeavours to ensure that procedures, rules and safeguards are in place for **remote learning**.

4.8 The Trust actively encourages a proactive approach to new and emerging technologies and threats to mitigate the risk of harm to students and staff and the trust and associated academies and their reputations. The Trust seeks to promote a cyber-awareness culture that ensures all staff, students and governors take part in and continue to develop their knowledge and understanding of online behaviours and in particular, how to prevent harm through continual learning resources, research and encouragement from all teachers.

5. Who is responsible for online safety and what are their responsibilities?

5.1 The Trust:

- Takes overall responsibility for data management and information security ensuring provision follows best practice in information handling; work with all relevant parties to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Provides support to schools so they can ensure effective use of appropriate IT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Ensures processes are in place for **remote-learning** procedures, rules and safeguards.
- Reviews and updates this policy, Acceptable Use Policies and other procedures on a regular basis or as required.
- Provides school-safe filtering and monitoring, supplied by 'The ICT Service, Cambridgeshire'. The Smoothwall automated products monitor all keystrokes and report concerns to Trust and Academy staff.

5.2 Governors:

- The Safeguarding Governor and the DSL will liaise directly with one another with regard to report on online effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and wider school community.
- Ask about how the school has reviewed protections for **remote-learning** procedures, rules and safeguards.
- To ensure that they have demonstrable experience, skills and training to be able to provide appropriate challenge and support to the school management team.
- To provide and evidence a link between the school, governors and parents.

5.3 The Designated Senior Lead (DSL):

- Act as the named point of contact for all online safety incidents or issues and liaise with other members of staff and agencies as appropriate.
- Escalate online safety incidents to the relevant external parties e.g. CEOP, local Police, Local Safeguarding Children's Board, social services and parents/carers. Possible scenarios might include: Allegations against members of staff; Computer crime – hacking of school systems; Allegations or evidence of 'grooming' and Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.

- Keep up to date with current research, legislation and trends in online safety issues.
- Coordinate participation in local and national online safety events.
- Ensure that that that online safety is promoted to staff, students, parents and carers through a variety of channels and approaches. This may include facilitating regular assemblies, Wake Up Wednesday and other such activities that focus on positive messages and behaviours.
- Work with relevant staff to ensure that data protection and data security practice is in line with legislation.
- Maintain an online safety incident/action log to record incidents and actions taken as part of the Academy's safeguarding recording mechanism.
- Monitor online safety incidents to identify trends and patterns and update education response to reflect this need.
- Act 'in loco parentis' and liaising with websites and social media platforms, such as Twitter and Facebook, to remove instances of illegal material or cyber bullying.
- Ensure that online safety is integrated with other appropriate policies and procedures.
- Audit and assesses inset requirements for staff, support staff and governor online safety training
- Work with the relevant staff to review protections for **remote-learning** procedures, rules and safeguards.

5.4 Staff/contractors managing the technical environment:

- Provide and maintain a safe and secure technical infrastructure (including networks, infrastructure and hardware etc.) which supports safe online practices, ensuring learning opportunities are maximised.
- Ensure systems are not open to abuse or unauthorised external access.
- Be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure
- Defend the network and infrastructure of the academy, reviewing activity logs regularly
- Ensure that users comply with basic access policies and that only trusted devices can connect to the academy network
- Ensure that filtering of search facilities is robust and regularly checked for penetration to ensure that the risk of students accessing material that is unsuitable is minimised.
- To keep up to date with current threats and attack trends and take steps to mitigate this and communicate with the management team
- To report to the management team any network intrusions or other threats to the network
- To ensure that any IT outsourced e.g. connectivity, maintenance, cloud based services website, email provision, filtering, anti-virus, complies with DfE guidance and Data Protection regulations.
- Promoting basic cyber security practices within the academy e.g. locking computers when away from the desk, using secure passwords, caution when using USB removable drives.
- External contractors, website designers/hosts will be made fully aware of and agree to the Trust's Online Safety Policy.
- Provide technical support as required to ensure the development and implementation of appropriate online safety policies and procedures.
- Support home learning and remote teaching technologies as required.

5.5 All staff:

- Ensure they are aware of the current online safety policy, practices and associated procedures including those for reporting online safety incidents.
- Read, understand and follow the Acceptable Use Policy, and sign annually to say they have done so.

- Have an awareness of online safety issues and how they relate to the children in their care.
- Be provided with an online safety induction as part of the overall staff induction procedures.
- All staff will undertake safeguarding training as required including reading KCSIE part 1 and Annex A & C when requested to do so.
- Embed online safety education in curriculum delivery wherever possible.
- Promote and reinforce safe online practices when on and off-site, including providing advice to students on how to report incidents. This will be done through the curriculum and therefore requires the support of all staff. The RSHE curriculum will also form part of this. Encourage discussion about online learning issues in lessons, including appropriate behaviour online and how to get help.
- Pay particular attention to safeguarding provisions for online safety, home-learning and remote-teaching technologies.
- Model professional, safe and responsible behaviours in their own use of technology both on and off site.
- Check and document internet usage and suggested websites in lesson planning prior to teaching them.
- Be vigilant in monitoring student Internet and computer usage in line with the policy. This may include the use of personal technology, such as cameras, phones on the school site where there is a cause for concern.
- Know when and how to escalate online safety issues, internally and externally.
- Report as soon as is practicable any suspected misuse of Trust/academy digitally connected systems to the Principal, DSL or other relevant person.

5.6 PSHE Leads:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE /Relationships Education, Relationships and Sex Education (RSE) and Health Education curriculum.

  "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."

- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Pay particular attention to safeguarding provisions and online safety for home-learning and remote-teaching technologies.

5.7 Children and young people:

- Read the Academy's Acceptable Use Policy and adhere to them.
- Respect the rights and feelings of others both on and offline.
- Seek help from a trusted adult or support network if things go wrong and support others who may be experiencing online safety issues. Examples may include a member of staff, CEOP, Child line etc.
- Contribute to the development of online safety and Acceptable Use policies through Student Voice.

- Be aware of and comply with academy policies for Internet and mobile technology usage in the academy, including the use of personal items such as mobile phones.
- Follow basic cyber security practices within the academy e.g. locking computers when away from the desk, using secure passwords etc.
- Be aware that their Internet use out of school on social networking sites is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and students in terms of cyber bullying, reputation or illegal activities.

And at a level that is appropriate to the individual age, ability and vulnerabilities:

- Sign the Academy's Acceptable Use Policy.
- Take responsibility for keeping themselves and others safe online.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assess the personal risks of using any particular technology and behave responsibly to limit those risks.
- Work with the relevant staff to follow **remote-learning** procedures, rules and safeguards.

5.8 Parents and carers:

- Read their child's academy's Acceptable Use Policy and support and encourage them to adhere to it and to adhere to it themselves as needed.
- Sign the academy's Acceptable Use Policy, indicating agreement regarding their child's user and also their own use with regard to parental access to school systems such as websites, forums, social media, online reporting arrangements and questionnaires.
- Discuss online safety issues with their children, supporting the academy in their online safety approaches and reinforcing appropriate safe online behaviours at home.
- Role model safe and appropriate uses of new and emerging technology.
- Identify changes in their child's behaviour which indicate that their child is at risk of harm online.
- Seek help and support from the academy, or other appropriate agencies, if they have concern.
- Use school systems safely and appropriately.
- Take responsibility for their own awareness and learning in relation to online risks for their children.

6. Procedures

6.1 Systems

6.1.1 School computer systems will be configured to ensure the teaching and learning requirements of the school are met whilst ensuring online safety is maintained.

6.1.2 Risk assessments are completed when there is a major overhaul to the system or a new cloud-based software package is purchased, for example.

6.1.3 The system will be compliant with the Academy, Trust, local authority, DfE, ICO and Data Protection guidelines with regard to online safety procedures being met.

6.1.4 Regular audits and evaluations of the IT network will be carried out, identifying where improvements can be made.

6.1.5 IT use will be monitored.

6.2 Filtering

6.2.1 The academy will ensure an accredited filtering system is used. Filtering reports and logs will be examined regularly.

6.2.2 Any filtering incidents are examined and action taken and recorded to prevent a reoccurrence.

6.2.3 The academy will provide enhanced/differentiated user-level filtering. Internet access will be filtered for all users.

6.3 Network security

6.3.1 All users will have clearly defined access rights to academy technical systems and devices.

6.3.2 All users will be provided with a username and secure password by School IT staff. Users are responsible for the security of their username and password.

6.3.3 The Network Manager and Principal/other designated senior person will have access to the main administrator password.

6.3.4 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

6.4 Use of images and videos

6.4.1 The academy will ensure images and videos of students, staff, students' work and any other personally identifying material are used, stored, archived and published in line with the Data Protection Act, ICO guidance for schools, DfE guidance for schools and the Acceptable Use Policy.

6.4.2 When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images, in particular the risks attached to publishing their own images on the Internet e.g. social media sites.

6.4.3 Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press.

6.4.4 In accordance with guidance from the ICO, parents/carers are able to take videos and digital images of their children at academy events for their own personal use, but should not be made publicly available where other students are involved in the digital image or video.

6.4.5 Students must not take, use, share, publish or distribute images of others without their permission.

6.5 Data Protection

6.5.1 Personal data will be recorded, processed, transferred and made available according to the Trust Data Protection Policy (TPO/STA/25) and in compliance with the Data Protection Act (2018).

6.6 Social Media

6.6.1 Governors, staff, students and volunteers are expected to comply with the Trust Social Media Policy (TPO/STA/20).

6.7 Managing email

6.7.1 Pupils, staff and governors may only use their academy/Trust email accounts for educational purposes and for any official communication. The use of personal email addresses for any official business is not permitted.

6.7.2 Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods. Only data that needs to be shared should be.

6.7.3 Members of the school community must report any offensive communication immediately to the DSL.

6.7.4 Emails sent internally should be professionally written and only used if there is no better way to communicate information. This is important in managing staff workload.

6.7.5 Emails sent to external organisations should be written carefully and authorised before sending, in the same way that a letter written on school headed paper would be.

6.7.6 Each academy will have a dedicated email for reporting wellbeing and pastoral issues. The inbox should be managed by designated and trained staff.

6.7.7 School email addresses must not be used for setting up personal social media accounts.

7. Educating students about online safety - curriculum

7.1 Students will be taught about online safety as part of the curriculum.

7.2 In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they will know:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

The safe use of social media and the internet will also be covered in other subjects where relevant.

Academies will use a range of activities to raise pupils' awareness of the dangers that can be encountered online including assemblies, Awareness Days, external speakers etc.

8. Educating parents and carers about online safety

8.1 The Trust recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and digital technology. In 2020-21 it is even more important that parents and carers support their children with the procedures, rules and safeguards that are in place for **remote learning** as the level of education that has to take place at home may increase due to the COVID-19 pandemic.

8.2 Academies will raise parents' and carers' awareness of internet safety in letters or other communications home, and in information via the website. This policy will also be shared with parents.

8.3 Parents and carers are requested to read the academy's Acceptable Use Policy for Students and discuss it with their children. We also request parents read and discuss online safety information as part of the Home School Agreement with their children.

8.4 If parents have any queries or concerns in relation to online safety or this policy, these should be raised in the first instance with the Principal and/or the DSL.

9. Use of mobile phones

9.1 Each Academy will have its own approach to the use of mobile phones in school. This will be clearly communicated to students, staff, parents/carers and volunteers.

9.2 Any use of mobile phones must be in line with the relevant acceptable use agreements.

9.3 Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the Behaviour Policy, which may result in the confiscation of their device.

10. Policy Review

10.1 This policy will be monitored as part of the Academy's annual internal review and reviewed annually or as required by legislation changes.

10.2 An up to date copy of the policy will be available on the Trust website.

Document Control

Date of last review:	September 2021	**Author:**	Special Projects Lead and Trust Safeguarding Officer
Date of next review:	September 2022	**Version:**	3
Approved by:	Strategic Delivery Group	**Status:**	Ratified

Summary of Changes

- Inserted under principles the online safety risks categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce ***(paragraph 1.4)***.
- Inserted school-safe filtering and monitoring provider information and reporting to the Trust and academy staff ***(paragraph 5.1)***.

Appendix A – Responding to inappropriate online incidents and concerns

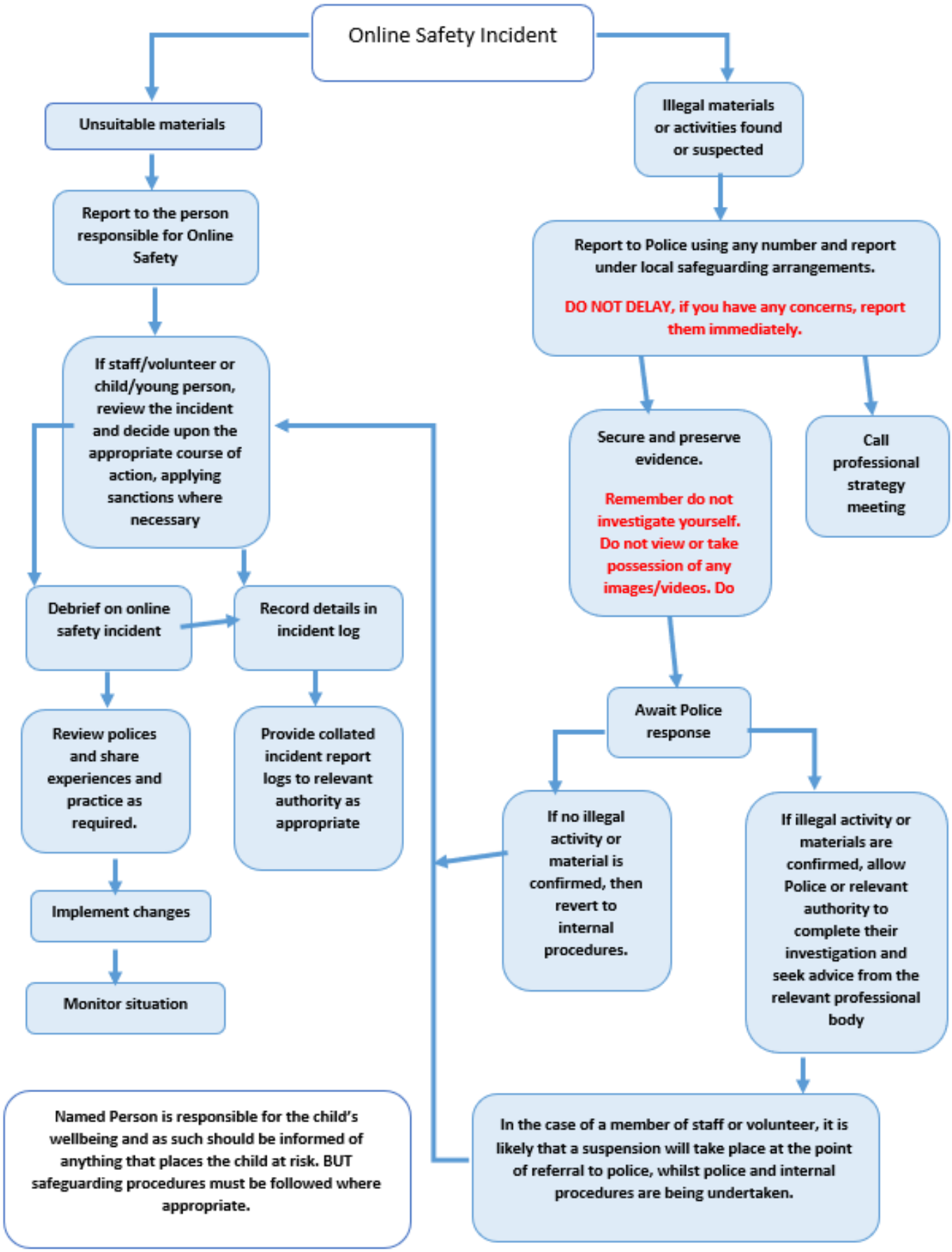
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school/academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range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

The Trust believes that the activities referred to in the following section are inappropriate in an education context and that users, as defined below, must not engage in these activities in/or outside the school/academy when using academy equipment or systems. The school/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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices						X

• Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				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		

NB It is essential that any relevant procedures in the Safeguarding and Child Protection Policy are also followed, which may include referrals to the Local Authority Designated Officer and/or the Police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await 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 at the point of referral to police, whilst police and internal procedures are being undertaken.

It is more likely that Academy's 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 school 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:

NB All should be logged on CPOMS and Safeguarding Team will refer to the relevant person.

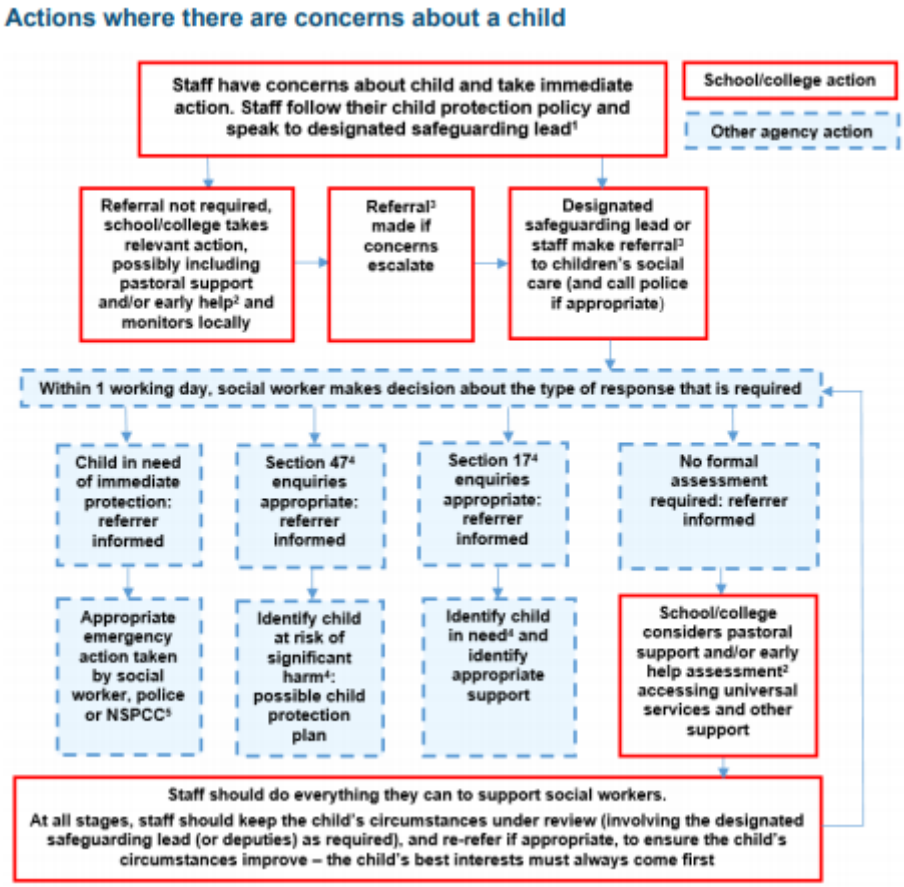
Students/Pupils Incidents	Refer to class teacher/tutor	Refer to Head of Year	Refer to Principal	Refer to Police	Refer to technical support staff	Further sanction	Intervention
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X		X	
Unauthorised use of non-educational sites during lessons	X	X			X		
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device		X	X	X	X	X	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email		X					X
Unauthorised downloading or uploading of files		X				X	
Allowing others to access school/academy network by sharing username and passwords		X					
Attempting to access or accessing the school/academy network, using another student's/pupil's account		X				X	
Attempting to access or accessing the school/academy network, using the account of a member of staff			X			X	
Corrupting or destroying the data of other users		X				X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X	X
Continued infringements of the above, following previous warnings or sanctions			X			X	X

Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school			X			X	
Using proxy sites or other means to subvert the school's/academy's filtering system			X			X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X	X
Deliberately accessing or trying to access offensive or pornographic material			X			X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X	X

Staff 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.		Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal		X	X	X			X
Inappropriate personal use of the internet/social media/personal email		X					X
Unauthorised downloading or uploading of files		X			X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X					X
Careless use of personal data e.g. holding or transferring data in an insecure manner		X			X		X
Deliberate actions to breach data protection or network security rules		X			X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X					X

Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		X					
Actions which could compromise the staff member's professional standing		X					X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy		X					
Using proxy sites or other means to subvert the school's/academy's filtering system		X					
Accidentally accessing offensive or pornographic material and failing to report the incident		X					
Deliberately accessing or trying to access offensive or pornographic material		X					X
Breaching copyright or licensing regulations		X					
Continued infringements of the above, following previous warnings or sanctions		X					X

All are reminded of the duty to actions to take where there are concerns about a child as outlined in Keeping Children Safe in Education 2020.



Appendix B – Responding to online incidents and concerns: Self-Generated Indecent Images of Children (Sexting)

There is no clear definition of 'sexting' and it can mean different things to different people. However, in the context of schools and young people, this guidance refers to sexting to mean 'youth produced sexual imagery' as this is the definition set out by the UK Council for Child Internet Safety (UKCCIS). Within this definition:

- 'Youth' refers to anyone under the age of 18.
- 'Youth produced' includes young people sharing images that they, or another young people, have created of themselves.
- 'Imagery' covers both still photos and moving videos.

Self-Generated Indecent Images of Children (SGIIOC or "Sexting") are therefore images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. These images may be shared between children and young people and/or adults via a mobile phone, webcam, handheld device or website. It is more common in older children and teenage years where they are becoming more sexually aware and going through puberty. It is a safeguarding issue.

Young people typically do not use the term "sexting", usually referring to the images as "nudes" and may decide to send such pictures or videos for many reasons. For younger children (early years and primary school aged) indecent images or videos may be taken or shared out of curiosity or naivety and for older children, indecent images may be taken or shared as a response to peer pressure, cyberbullying, sexual exploration, impulsive behaviour, "flirting" or even exploitation due to blackmail from a friend, partner, or other on or offline contact.

A NSPCC survey in 2016 found that 13% of boys and girls had taken topless pictures of themselves (around one in four of those were girls) and 3% had taken fully naked pictures.

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to take an indecent photograph or allow an indecent photograph to be taken, make an indecent photograph (this includes downloading or opening an image that has been sent via email); distribute or show an indecent image, advertise indecent images and possess an indecent image or possess an indecent image with the intention of distribution. This applies even if the images are sent or shared by someone under the age of 18 with "consent". "Sexts" may be viewed as police evidence and it is essential than schools secure devices and seek advice immediately when dealing with concerns.

The current Association of Chief Police Officers (ACPO) position is that:
'*ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children especially if they are convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.'*
www.ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO_Lead_position_on_Self_Taken_Images.pdf

The prosecution for sharing indecent images for a first offence is unlikely. Wider vulnerability considerations for all of those involved should always be made and pastoral and wellbeing measures are likely to have more impact in stopping repeat behaviour. External support from an appropriate agency can be sought when required.

The impact of intimate photos being shared is immense – isolation, bullying, poor mental health (low self-esteem, low mood, self-harm etc.), reputational damage and increased risk of CSE. Academies should take steps to ensure

that children and young people are aware of the risks and that staff know what to do should they become aware of such an incident.
'Sexting' incidents need to be handled as carefully as possible and support offered to all. Schools and settings must NOT print/copy etc. images suspected to be indecent – the device should be secured until advice can be obtained.

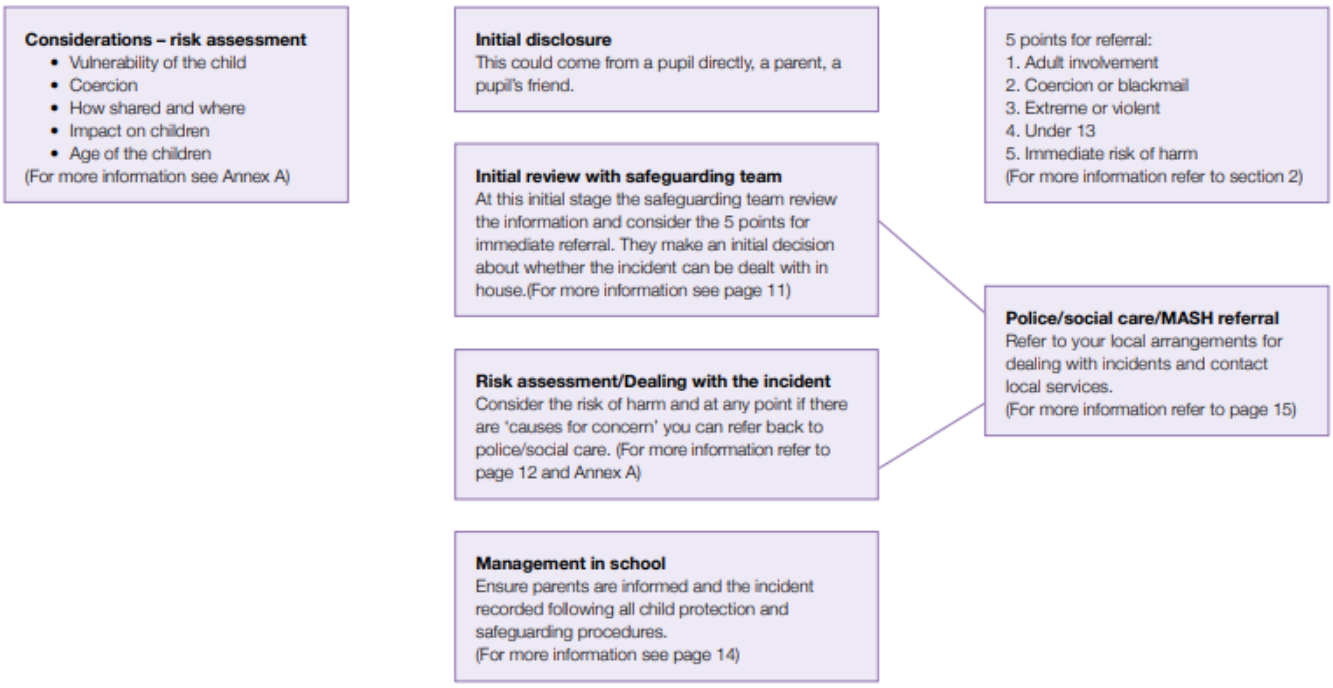
Further guidance can be found at
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759007/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

The following statements may enable academies to consider how best to respond to concerns relating to 'sexting':

- What is the age of the child(ren) involved?
  - If under 13 then a consultation/referral to Children's Social Care should be made.
  - If an adult (over 18) is involved, then consider using the KSCB CSE toolkit.
- Is there any contextual information to help inform decision making?
  - Are the children involved in a relationship and if so is the relationship appropriate?
  - Is this age appropriate experimentation, natural curiosity or possible exploitation?
- Is the school or other agencies (e.g. Police or social care) aware of any vulnerability for the children(s) involved?
  - Special education needs, emotional needs, children in care, youth offending?
- Are there any other risks or concerns known by the school or other agencies which may influence decisions or judgements about the safety and wellbeing of the child(ren) involved?
  - Family situation, children at risk of sexual exploitation?
- How were the school made aware of the image?
  - Did a child disclose about receiving, sending or sharing an image themselves or was the concern raised by another pupil or member of the school community?
- What sort of image is it?
  - Is the image potentially illegal or is it inappropriate?
- Does the child(ren) know who has accessed the image?
  - Was it sent to a known peer (e.g. boyfriend or girlfriend) or an unknown adult?
  - Do they know where the image has been shared?
  - Has it been shared online or sent to another child/person?
- How widely has the image been shared?
  - Just to one other child or to an unknown number of children/adults?
- Are there other children/pupils involved?
  - If so, who are they and are there any safeguarding concerns?
  - What are their views/perceptions on the issue?
- What apps, services or devices are involved (if appropriate)?
  - Some apps and devices may automatically store, backup or delete images which can influence evidence gathering.
- Is the image on a school device or a personal device? Is the device secured?
- Does the child need immediate support and or protection?
  - What is the impact on the child?
  - What can the school put in place to support them?
- Are other schools/settings involved?
  - Does the relevant Designated Safeguarding Lead need to be identified and contacted?
- Is this a first incident or has the child(ren) been involved in sexting concern before?
  - If so, what action was taken and does this possibly increase concerns for offending behaviour?
- Are the school child protection and safeguarding policies and practices being followed?

The flowchart below indicates how academies should respond to 'sexting'.

Flowchart for responding to incidents



Appendix C – Responding to online incidents and concerns: Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, each academy will ensure that students understand what it is and what to do if they become aware of it happening to them or others. They will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Each academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Academy staff will discuss cyber-bullying with their students, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, each academy will follow the processes set out in the Behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Investigations into cyberbullying should be those as outlined in the Anti-bullying policy and peer on peer abuse policy.

Appendix D – Responding to online incidents and concerns: Online child sexual abuse

Online child sexual abuse is defined as when children are sexually abused or exploited via the use of technology and the internet. This can be referred to as "online grooming" however this term can be considered too narrow as it can happen over a short as well as long time scale, where trust is developed.

In 2015, CEOP identified that the objectives of online child sexual abuse have evolved and can lead to a range of offending outcomes, such as deceiving children into producing indecent images of themselves or engaging in sexual chat or sexual activity over webcam. Online child sexual abuse can also result in offline offending such as meetings between an adult and a child for sexual purposes following online engagement. Online child sexual abuse can also be perpetrated by young people themselves and these issues should be viewed and responded to in line with the Local Safeguarding Children Board procedure for children who display harmful behaviours.

Online child sexual abuse is a safeguarding issue. It can also link in with Child Sexual Exploitation.

All Academy's will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns. Action regarding online child sexual abuse will be taken regardless of the use of school equipment or personal equipment, both on and off the school premises.

Preventative measures will take place through education and training.

Child Exploitation Online Protection Command is a command of the UK's National Crime Agency (NCA),[1] and is tasked to work both nationally and internationally to bring online child sex offenders, including those involved in the production, distribution and viewing of child abuse material, to the UK court. The CEOP report button is visible and available to pupils and other members of the school community, for example on the schools website.

Action to take:

When staff become aware of an incident, the Safeguarding and Child Protection Policy and LCSB procedures must be followed

1) It must be logged on CPOMS and/or reported to the DSL immediately. The Safeguarding Team will then take relevant action.
2) Store any devices involved securely.
3) Immediately inform local police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
4) Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse.
5) Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
6) Make a referral to children's social care (if needed/appropriate).
7) Put the necessary safeguards in place for pupil(s).
8) Inform parents/carers about the incident and how it is being managed.
9) Support and intervention put in place.
10) Further Guidance from the Police, MASH and Local Authority will be sought as required.
11) Review the handling of any incidents to ensure best practice and make any revisions required.

.

Appendix E – Responding to online incidents and concerns: Indecent images of children

The Sexual Offences Act 2003 defines a child as under the age of 18. It is an offence to possesses, distribute, show and make indecent images of children, this includes printing and viewing or 'downloading'.

Where there is concern that **illegal activity** (whether it be student or staff) has happened the following steps should be taken as soon as possible:

- Ensure the DSL is informed immediately or other member of staff in accordance with the Whistleblowing Policy
- Quarantine and store any devices and evidence securely
- Determine if the concern is within the school's remit. If it is not, it must be reported to the Police as soon as possible. If the DSL is unsure the Police or MASH must be contacted
- The Local Authority Designated Officer (DO) must also be contacted if the concern is about a member of staff.
- The advice of these external agencies should be followed
- Report any webpages e.g. Internet Watch Foundation (https://www.iwf.org.uk/)
- Only store copies of images securely (where they can only be accessed by the Safeguarding Team) at the request of the police
- Follow the relevant Trust policies regarding conduct (whether they be student or staff).

In all cases a detailed statement must be written including:

  - The identity of any involved including witnesses and their detail (email address, screen names etc.)
  - The name of the ISP or mobile service provider
  - The web address, app or website through which the image was found
  - Any passwords or other procedures used to access the image
  - The identity of the person who sent the image
  - If there is any delay in reporting to the police the reason why
  - The outcome.

These statements should be securely stored.

If there is concern that a member of staff or student has been **inadvertently exposed** to indecent images:

- Ensure the DSL is informed
- Seek guidance from the police/MASH/DO as required
- Report any webpages e.g. Internet Watch Foundation (https://www.iwf.org.uk/)
- Delete any copies of the image after police advice sought.

If there is concern that indecent images **have been found** on the schools electronic devices/system:

- Ensure the DSL is informed
- Inform the police/MASH as appropriate
- Report any webpages e.g. Internet Watch Foundation (https://www.iwf.org.uk/)
- Delete any copies of the image after police advice sought.

NB Sexting images will be managed as per Appendix B

Appendix F – Responding to online incidents and concerns: Radicalisation

All Academy's need to be aware of their roles and responsibilities as set out in the Prevent Duty: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

All staff need to understand the early warning signs and inform the DSL using CPOMS of any concerns.

The DSL and safeguarding team must understand when a referral to the Channel Programme may be necessary. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/928326/6.6271_HO_HMG_Channel_Duty_Guidance_v13_WEB_Engish.pdf

All academies must share information and work together with partner agencies as required.

Appendix G – Cyber Crime

https://www.npcc.police.uk/documents/Children%20and%20Young%20people/When%20to%20call%20police%20guidance%20for%20schools%20and%20colleges.pdf

Cybercrime is criminal activity committed using computers and/or the internet. It can involve malicious attacks on computer software, including:

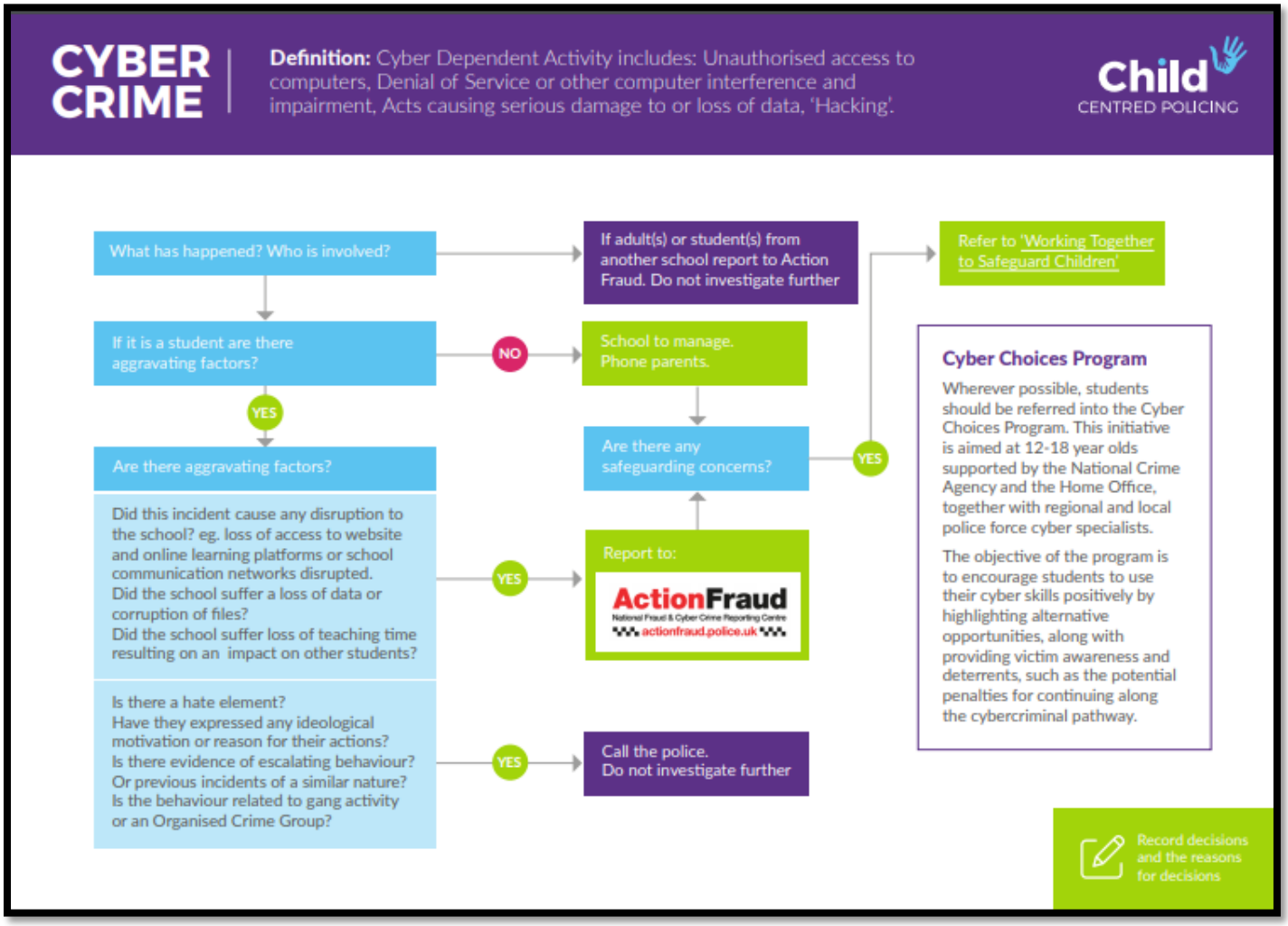
- Breaking IT rules
- Unauthorised access to computers
- Denial of Service or other computer interference and impairment
- Acts causing serious damage to or loss of data
- 'Hacking'
- Cheating at online gaming

This guidance has a focus on offences committed by young people rather than external cybercrime and cyber security for which further guidance can be found at www.ncsc.gov.uk

The Academy should first establish:

- What has happened?
- Who is involved?
- Is this part of a pattern of behaviour?
- Are there any safeguarding concerns? If YES — Refer to Keeping Children Safe In Education (September 2020) and follow local safeguarding protocols
- Are there any aggravating factors?
- Did this incident cause any disruption to the school? E.g. loss of access to website and online learning platforms or school communication networks disrupted.
- Did the school suffer a loss of data or corruption of files?
- Did the school suffer loss of teaching time resulting on an impact on other students?
- Is there a hate element?
- Have they expressed any ideological motivation or reason for their actions?
- Is there evidence of escalating behaviour? Or previous incidents of a similar nature?
- Is the behaviour related to gang activity or an Organised Crime Group?
- Do the young people involved have any additional relevant vulnerabilities?

Action should then be taken as per the flow chart below:


CYBER CRIME
Definition: Cyber Dependent Activity includes: Unauthorised access to computers, Denial of Service or other computer interference and impairment, Acts causing serious damage to or loss of data, 'Hacking'.
Child CENTRED POLICING
What has happened? Who is involved?
If adult(s) or student(s) from another school report to Action Fraud. Do not investigate further
Refer to 'Working Together to Safeguard Children'
If it is a student are there aggravating factors?
NO
School to manage. Phone parents.
YES
Are there aggravating factors?
Are there any safeguarding concerns?
YES
Did this incident cause any disruption to the school? eg. loss of access to website and online learning platforms or school communication networks disrupted.
Did the school suffer a loss of data or corruption of files?
Did the school suffer loss of teaching time resulting on an impact on other students?
YES
Report to:
ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk
Is there a hate element?
Have they expressed any ideological motivation or reason for their actions?
Is there evidence of escalating behaviour?
Or previous incidents of a similar nature?
Is the behaviour related to gang activity or an Organised Crime Group?
YES
Call the police.
Do not investigate further
Cyber Choices Program
Wherever possible, students should be referred into the Cyber Choices Program. This initiative is aimed at 12-18 year olds supported by the National Crime Agency and the Home Office, together with regional and local police force cyber specialists.
The objective of the program is to encourage students to use their cyber skills positively by highlighting alternative opportunities, along with providing victim awareness and deterrents, such as the potential penalties for continuing along the cybercriminal pathway.
Record decisions and the reasons for decisions

Appendix H – Relevant 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 online 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.

Academies may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

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.

The Data Protection Act 2018:
Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

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, 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 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. (see template policy in these appendices and for DfE guidance - 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)

Criminal Justice and Courts Act 2015
Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Appendix I - Online Safety guidance and resources

Statutory Guidance:

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912592/Keeping_children_safe_in_education_Sep_2020.pdf
- https://www.gov.uk/government/publications/preventing-and-tackling-bullying
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759007/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/928326/6.6271_HO_HMG_Channel_Duty_Guidance_v13_WEB_Engish.pdf
- https://www.gov.uk/government/publications/searching-screening-and-confiscation
- The current OFSTED Inspection Frameworks

Helpful websites and information

- https://nationalonlinesafety.com/about
- https://www.ceop.police.uk/safety-centre/
- https://www.npcc.police.uk/documents/Children%20and%20Young%20people/When%20to%20call%20police%20guidance%20for%20schools%20and%20colleges.pdf
- https://www.iwf.org.uk/
- https://www.actionfraud.police.uk
- https://www.lucyfaithfull.org.uk/
- https://www.mariecollinsfoundation.org.uk/

For parents

- https://www.ceop.police.uk/safety-centre/
- https://www.thinkuknow.co.uk/
- https://educateagainsthate.com/parents/
- https://nationalonlinesafety.com/guides
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting
- https://www.internetmatters.org/
- https://www.net-aware.org.uk/

For students

- https://www.thinkuknow.co.uk
- https://www.ceop.police.uk/safety-centre
- www.childline.org.uk

Curriculum

- https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf