ST PAUL'S CHURCH OF ENGLAND PRIMARY SCHOOL & NURSERY

# Online Safety

| | |
|---|---|
| Updated by | Miss Jones |
| Updated when | September 2024 |
| Ratified by | Safeguarding Governor |
| Ratified when | September 2024 |
| Signed by | C Zittel |
| Next Review Date | September 2025 |
| Statutory Policy | n/a |
| On school website | Yes |

| | | | | |
|---|---|---|---|---|
| **COURAGE** | **RESPECT** | **HOPE** | **ENJOYMENT** | **COMMUNITY** |

**Development, Monitoring and Review of this Policy**
This E-Safety policy has been developed in conjunction with the Headteacher, Governors, staff and pupils and is communicated to parents online. In light of the fast-moving development of information technology, this policy will be reviewed annually and shared with all members of the school community.

**Scope of the Policy**
This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school's ICT systems, both in and out of the school. This includes the use of Microsoft Teams and Class Dojo for in school use, home learning and remote learning.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying or other online safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that takes place out of school.

**Roles and Responsibilities**
The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

<u>Governors:</u>
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The role of E-Safety Governor is combined with that of the Child Protection / Safeguarding Governor. The role of the E-Safety Governor will include:

- Regular meetings between E-Safety Governor and HT regarding e-safety within the Safeguarding remit
- Attendance at E-Safety/Safeguarding meetings
- Regular monitoring of online safety incident logs recorded on CPOMS
- Regular monitoring of filtering
- Reporting to relevant Board meetings

<u>Headteacher:</u>
The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.

The Headteacher, the DSLs and DDSLs within the SLT are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

<u>E-Safety Co-ordinator (DSL/HT):</u>
The role of the E-Safety Co-ordinator is combined with the role of the DSL and will:

- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provide training and advice for staff
- Liaise with the local authority

- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- Meet regularly with the online safety governor to discuss current issues, review incident logs and filtering
- Attend relevant meetings of governors

Network Manager:
The role of the Network Manager is taken on by the Bursar who is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and local authority E-safety policy or guidance that may apply
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher for investigation
- That monitoring software and systems are implemented and updated as agreed in school policies

Teaching and Support Staff:
Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school E-Safety Policy and practices
- They report any suspected misuse or problem to the Headteacher for investigation
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the E-Safety procedures
- They monitor the use of digital technologies, mobile devices, cameras etc. In lessons and other school activities and implement current policies with regard to these devices
- They monitor the use of Microsoft Teams both in school and work sent in from home.
- They monitor the use of Class Dojo both in school and Nursery and work sent in from home.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead and Deputy Designated Safeguarding Leads:
The DSLs and DDSLs are trained in E-Safety issues and are aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyberbullying

These are safeguarding issues, not technical issues; it is simply that the technology provides additional means for safeguarding issues to develop.

Pupils:

- Are responsible for using the school digital technology systems in accordance with safe practice
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand procedures on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyberbullying
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

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

**Policy Statements**

Education – Students / Pupils:

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

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

- A planned online safety curriculum is provided as part of Computing, PSHE and other lessons.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Education – Parents / Carers:

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

The school therefore seeks to provide information and awareness to parents and carers through:

- Curriculum activities
- Newsletters, website, emails
- Parents / Carers evenings / sessions
- Events / campaigns e.g. Safer Internet Day

Technical – Infrastructure / Equipment, Filtering and Monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Bursar who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place (eg school / academy safe).
- The Bursar is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Mobile Technologies and Use of Digital Photography

Mobile technology devices may be school owned / provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet.

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

Staff and volunteers are allowed to bring personal mobile devices into school and for these to be left on but on silent. Mobile devices should not be brought out and used in the presence of any

pupils at any time. In exceptional circumstances, for instance if the leader on a school trip needs to contact the school, use of a mobile device in the presence of pupils is permitted.

Pupils who bring mobile devices into school are to hand these into the School Office at the beginning of the school day. It can then be collected at the end of the school day.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

Use of photos of pupils for school communication such as the school website, newsletters and through local newspapers is permitted through parental permission on admission to the school. A list of children whose photos should not be used in this way, is held by the School Office.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images. The school reserves the right, however, to request that parents do not take photos or video if there is a child protection issue.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

<u>Dealing with Sexting Incidents</u>
Sexting is defined as the creating, possessing and sharing of sexual images, video and streaming by a person under 18. The response should be guided by the 'principle of proportionality'. "The primary concern at all times should be the welfare and protection of the young people involved" (Sexting in Schools and Colleges, UKCCIS). See Appendix for updated guidance.

Record all incidents of sexting in line with Safeguarding procedures, including both the actions you did take as well as the actions you didn't take and give justifications. In applying judgement to each incident, consider the following:

- Is there a significant age difference between the sender / receiver involved?

- Is there any external coercion involved or encouragement beyond the sender / receiver?
- Do you recognise the child as more vulnerable than usual i.e. at risk?
- Is the image of a severe or extreme nature?
- Is the situation isolated or has the image been more widely distributed?
- Are there other circumstances relating to either sender or recipient that may add cause for concern i.e. difficult home circumstances?
- Context.

If any of these circumstances are present, then do escalate or refer the incident using our normal child protection procedures. This includes reporting to the police. Record the details of the incident, action and resolution.

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998, which states that personal data must be:

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

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "privacy notice" and lawfully processed in accordance with the "conditions for processing"
- It has a data protection policy
- It is registered as a data controller for the purposes of the data protection act (DPA)

Staff must ensure that they:

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

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

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, once it has been transferred or its use is complete

**Communications**

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school:

- Ensuring that personal information is not published.
- Training is offered including: acceptable use; social media risks; checking of settings; data protection; reporting issues.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school.

**Unsuitable / Inappropriate Activities**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyberbullying 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 context, either because of the age of the users or the nature of those activities.

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

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003 | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation). Contrary to the Public Order Act 1986 | | | | | X |
| | Pornography | | | | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | Threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | Promotion of extremism or terrorism | | | | X | |
| | Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |
| Using school systems to run a private business | | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy | | | | | X | |

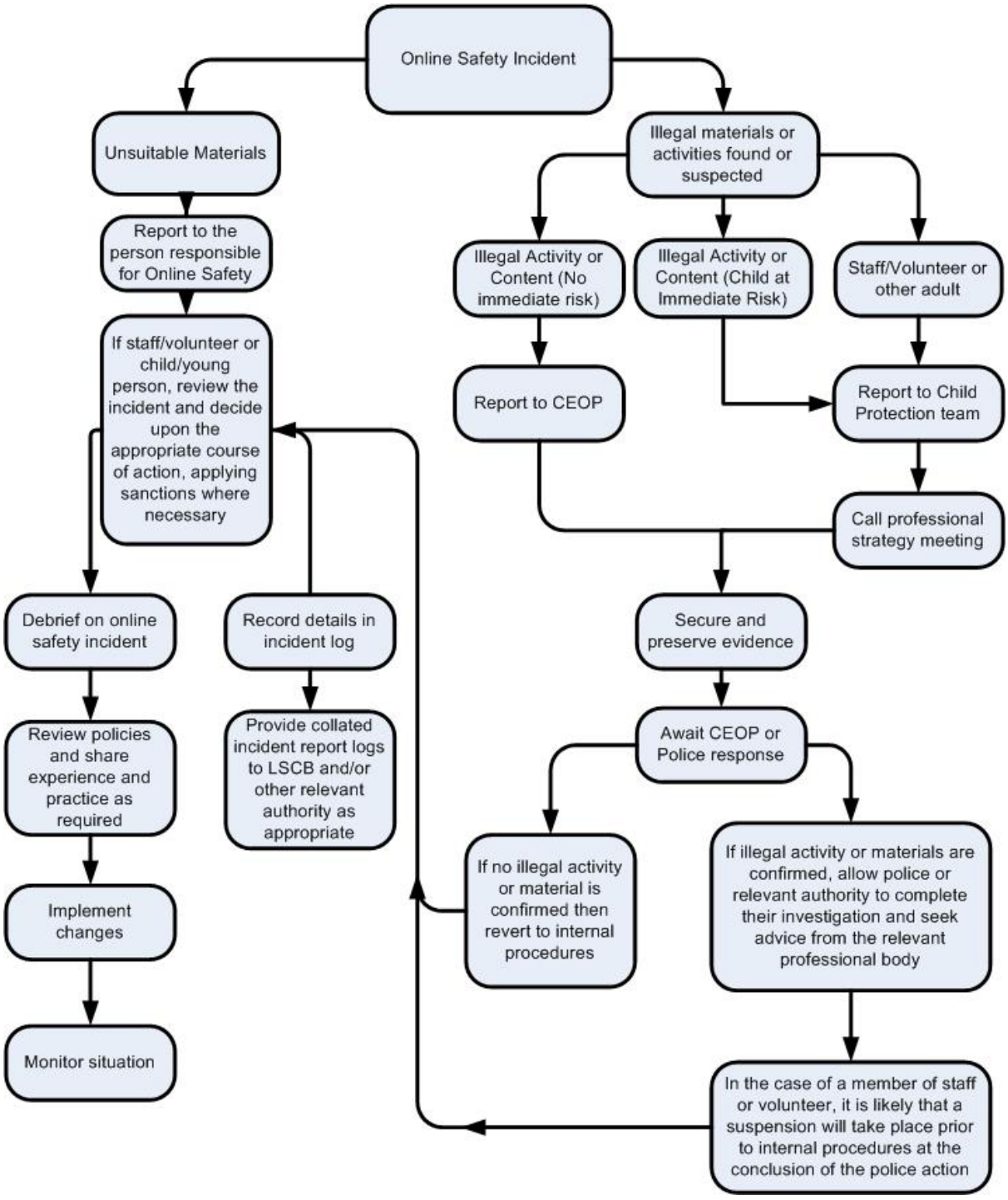
| | | | | | |
|---|---|---|---|---|---|
| Infringing copyright | | | | X | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | X | |

Responding to incidents of misuse

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

Illegal Incidents

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


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

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

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

- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the obscene publications act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions & Sanctions

It is more likely that the school 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 procedure.

# Pupil Acceptable Use Agreement Policy

School Policy

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

This Acceptable Use Agreement is intended to ensure:

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

# KS2 Pupil Online Acceptable Use Agreement

***This agreement will help keep me safe and help me to be fair to others***

- ***I am an online digital learner*** – I use the school's internet and devices for schoolwork, home learning and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.
- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.
- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

**I have read, understood and agree to this agreement. I know who are my trusted adults are.**

Child's name:_____ Year:_____

Child's signature:_____ Date:_____

## Key Stage 1: Acceptable Use Agreement

This is how I keep **SAFE online**:

| | |
|---|---|
| 1. I only use the devices I'm **ALLOWED** to | ✓ |
| 2. I **CHECK** before I use new sites, games or apps | |
| 3. I **ASK** for help if I'm stuck | |
| 4. I **THINK** before I click | |
| 5. I **KNOW** people online aren't always who they say | |
| 6. I don't keep **SECRETS** just because someone asks me to | |
| 7. I am **RESPONSIBLE** so never share private information | |
| 8. I **TELL** a trusted adult if I'm worried, scared or just not sure | |
| 9. I **KNOW** that if I break the rules I might not be allowed to use a computer/tablet | |

**My trusted adults are _____ at school and _____ at home.**

**My name is _____ in Year_____**

## Parent / Carer Acceptable Use Agreement

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

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the Home School Agreement to show their support of the school including this important aspect of the school's work.

## Parent / Carer Permission Form

Parent / Carer Name: ……..

Student / Pupil Name: ……..

Either: (KS2)
I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: …….

Date: …….

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

Group: ……

Date: ……

Reason for investigation:

……

……

……

……

……

Details of first reviewing person

Name: ……

Position: ……

Signature: ……

Details of second reviewing person

Name: ……

Position: ……

Signature: ……

Name and location of computer used for review (for websites)

……

……

……..

.....

.....

| Website(s) address / device | Reason for concern |
|---|---|
| | |
| | |
| | |
| | |
| | |

Conclusion and Action proposed or taken

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

Reporting Log

Group: .....

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

## Links To Other Organisations Or Documents

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

UK Safer Internet Centre
Safer Internet Centre – http://saferinternet.org.uk
Childnet – http://www.childnet-int.org
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk
CEOP
CEOP - http://ceop.police.uk
ThinkUKnow - https://www.thinkuknow.co.uk
Cyberbullying
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Data Protection
Information Commissioners Office:
Your rights to your information – Resources for Schools - ICO
Guide to Data Protection Act - Information Commissioners Office
Guide to the Freedom of Information Act - Information Commissioners Office
ICO guidance on the Freedom of Information Model Publication Scheme
ICO Freedom of Information Model Publication Scheme Template for schools (England)
ICO - Guidance we gave to schools - September 2012 (England)
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
Professional Standards / Staff Training
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline
Working with parents and carers
Online Safety BOOST Presentations - parent's presentation
Connectsafely Parents Guide to Facebook
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

**Appendix 1**

**(Responding to sexting in schools and colleges – UKCCIS Guidance Sexting in schools and colleges, responding to incidents, and safeguarding young people, guidance from the UK Council for Child Internet Safety)**

In August 2016 the UK Council for Child Internet Safety (UKCCIS) published non-statutory guidance on managing incidents of sexting by under 18s. Over 200 organisations were involved in creating the guidance, including government and the DfE, children's charities, UK Safer Internet Centre, CEOP, police and teachers' groups.

The UKCCIS guidance is non-statutory, but should be read alongside 'Keeping Children Safe in Education'. It should be followed unless there's a good reason not to do so.

There is no clear definition of 'sexting'. Instead, this document talks about 'youth-produced sexual imagery'. This is imagery that is being created by under 18s themselves and involves still photographs, video and streaming. In the guidance, this content is described as sexual and not indecent. Indecent is subjective and has no specific definition in UK law.

Incidents covered by this guidance:

- Person under 18 creates a sexual image of themselves and shares it with another person under 18.
- A person under 18 shares an image of another under 18 with another person under 18 or an adult.
- A person under 18 is in possession of sexual imagery created by another person under 18.

Incidents not covered by this guidance:

- Under 18s sharing adult pornography.
- Under 18s sharing sexual texts without sexual imagery.
- Adults sharing sexual imagery of under 18s. (This is child sexual abuse and must always be reported to the police.)

**Response to incidents of youth produced sexual imagery**

The response should be guided by the 'principle of proportionality'. 'The primary concern at all times should be the welfare and protection of the young people involved.' (Sexting in schools and colleges: responding to incidents and safeguarding young people, page 8)

**The Law**

Making, possessing and distributing any imagery of someone under 18 which is indecent is illegal. This includes imagery of yourself if you're under 18.

Indecent is not definitively defined in law, but images are likely to be considered indecent is they depict:

- A naked young person
- a topless girl
- an image which displays genitals
- sex acts including masturbation
- indecent images may also include overtly sexual images of young people in their underwear

These laws weren't created to criminalise young people but to protect them.

Although sharing sexual images of themselves is illegal and risky, it is often the result of curiosity and exploration. Young people need education, support and safeguarding, not criminalisation. The National Police Chiefs' Council (NPCC) is clear that "youth-produced sexual imagery should be primarily treated as a safeguarding issue."

Schools may respond to incidents without involving the police. (However, in some circumstances, the police must always be involved.)

**Crime recording**
When the police are notified about youth-produced sexual imagery, they must record this as a crime. The incident is listed as a crime, and the young person is the suspect. This is, however, not the same as a criminal record.

Every crime reported to the police must have an outcome code. The NPCC, Home Office and the DBS have agreed a new outcome code for youth-produced sexual imagery.

Outcome 21: This outcome code allows the police discretion not to take further action if it is not in the public interest, even though there is enough evidence to prosecute.

Using this outcome code is likely to mean the offence would not appear on a future Enhanced DBS check, although not impossible, as that disclosure is a risk-based decision. Schools can be assured that the police have the discretion they need not to adversely impact young people in the future.

Handling incidents:
- Refer to the designated safeguarding lead.
- DSL meets with the young people involved.
- Do not view the image unless it is avoidable.
- Discuss with parents, unless there is an issue where that's not possible.
- Any concern the young person is at risk of harm, contact social care or the police.

Always refer to the police or social care if the incident involves:
- An adult
- Coercion, blackmail or grooming
- Concerns about capacity to consent (e.g. Sen)
- Images showing atypical sexual behaviour for the child's developmental stage
- Violent acts depicted
- Image shows sex acts and includes a child under 13
- A young person at risk of immediate harm as a result of the disclosure (for example, self-harm or suicide)

Once DSL has enough information, the decision should be made to deal with the matter in school, refer it to the police or to social care. All information and decision-making should be recorded in line with school policy. If the incident has been dealt within school, a further review should be held to assess risks.

Assessing the risks once the images have been shared:
- Has it been shared with the knowledge of the young person?
- Are adults involved in the sharing?
- Was there pressure to make the image?
- What is the impact on those involved?

- Does the child or children have additional vulnerabilities?
- Has the child taken part in producing sexual imagery before?

Viewing images:
Avoid viewing youth-produced sexual imagery. Instead, respond to what you have been told the image contains.

- If it is felt necessary to view, discuss with the Headteacher first.
- Never copy, print or share the image (it's illegal).
- View with another member of staff present.

Record the fact that the images were videoed along with reasons and who was present. Sign and date.

**Deleting images (from devices and social media)**
If the school has decided that involving other agencies is not necessary, consideration should be given to deleting the images.

It is recommended that pupils are asked to delete the images themselves and confirm they have done so. This should be recorded, signed and dated.

Any refusal to delete the images should be treated seriously, reminding the pupil that possession is unlawful.

Summary:

- New guidance for schools.
- Not "sexting", but "youth-produced sexual imagery".
- Although illegal, police involvement not always necessary.
- Images can be deleted and incident managed in school.
- Risk-based approach.

What to do next:

- Make sure your policy reflects this guidance.
- Make sure relevant staff understand what to do.

Download the document 'Sexting in schools and colleges UKCCIS August 2016'

Taken from Andrew Hall information