Swain House Primary School

Online Safety Including use of Electronic Devices Policy



**September 2025**

**This policy will be reviewed in September 2026**

**Contents:**

[Statement of intent](#_Statement_of_intent_1)

1. [Legal framework](#_Legal_framework_1)
2. [Roles and responsibilities](#_[Updated]_Roles_and)
3. [Managing online safety](#_[Updated]_Managing_online)
4. [Cyberbullying](#_[New]_Cyberbullying)
5. [Child-on-child sexual abuse and harassment](#_[New]_Peer-on-peer_sexual)
6. [Grooming and exploitation](#_[New]_Grooming_and)
7. [Mental health](#_[New]__Mental)
8. [Online hoaxes and harmful online challenges](#_Online_hoaxes_and)
9. [Cyber-crime](#_[New]_Cybercrime)
10. [Online safety training for staff](#_[Updated]_Online_safety)
11. [Online safety and the curriculum](#_[Updated]_Online_safety_1)
12. [Use of technology in the classroom](#_Use_of_technology)
13. [Use of electronic devices (including mobile phones)](#_Use_of_devices)
14. [Educating parents](#_Internet__access)
15. [Internet access](#_Internet_access_1)
16. [Filtering and monitoring online activity](#_Filtering__and)
17. [Network security](#_Network__security)
18. [Emails](#_Emails)
19. [Generative artificial intelligence (AI)](#_[New]_Generative_artificial)
20. [The school website](#_The_school_website)
21. [Remote learning](#_Remote_learning)
22. [Monitoring and review](#_Monitoring_and_review_1)

**Appendix**

1. Online Safety Incident Report Log
2. Acceptable Use Agreement for EYs and KS1
3. Acceptable Use Agreement for KS2
4. Acceptable Use Agreement for staff and governors

**Statement of intent**

Swain House Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

* **Content**: Being exposed to illegal, inappropriate or harmful material, e.g.
  + Pornography
  + Racism
  + Misogyny
  + Self-harm
  + Suicide
  + Discrimination
  + Radicalisation
  + Extremism
  + Misinformation
  + Disinformation, including fake news
  + Conspiracy theories
* **Contact**: Being subjected to harmful online interaction with other users, e.g.
* Peer to peer pressure.
* Commercial advertising.
* Adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
* **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g.
  + Making, sending and receiving explicit messages
  + Consensual and non-consensual sharing of nudes and semi-nudes
  + Sharing of pornography
  + Sharing other explicit images
  + Online bullying
* **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

# 1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

* Online Safety Act 2023
* Voyeurism (Offences) Act 2019
* The UK General Data Protection Regulation (UK GDPR)
* Data Protection Act 2018
* DfE (2025) ‘Filtering and monitoring standards for schools and colleges’
* DfE (2021) ‘Harmful online challenges and online hoaxes’
* DfE (2025) ‘Keeping children safe in education 2025’ (KCSIE)
* DfE (2023) ‘Teaching online safety in school’
* DfE (2022) ‘Searching, screening and confiscation’
* DfE (2025) ‘Generative artificial intelligence in education’
* Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)’
* UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’
* National Cyber Security Centre (2020) ‘Small Business Guide: Cyber Security’

This policy operates in conjunction with the following school policies:

* Allegations of Abuse Against Staff Policy
* Technology Acceptable Use Agreement for staff
* Technology Acceptable Use Agreement for pupils
* Cyber-security Policy
* Child Protection and Safeguarding Policy
* Child-on-child Abuse Policy
* Anti-Bullying Policy
* Staff Code of Conduct
* Behaviour Policy
* Disciplinary Policy and Procedure
* Data Protection Policy
* Prevent Duty Risk Assessment
* Remote Education Policy

# 2. Roles and responsibilities

The Governing Body will be responsible for:

* Ensuring that this policy is effective and complies with relevant laws and statutory guidance
* Reviewing this policy on an annual basis
* Ensuring their own knowledge of online safety issues is up-to-date
* Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals
* Ensuring school implements appropriate filtering and monitoring systems in place
* Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers
* Ensuring that the LMT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified
* Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them
* Ensuring compliance with the DfE’s ‘Meeting digital and technology standards in schools and colleges’, with particular regard to the filtering and monitoring standards in relation to safeguarding.

The Headteacher will be responsible for:

* Ensuring that online safety is a running and interrelated theme throughout the school’s policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
* Supporting the DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
* Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
* Ensuring online safety practices are audited and evaluated.
* Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
* Working with the DSL and ICT Strategic Group and Reboot to conduct termly light-touch reviews of this policy.
* Working with the DSL and Governing Body to update this policy on an annual basis.
* Appointing a member of the LMT as digital lead (DSL)

The DSL will be responsible for:

* Taking the lead responsibility for online safety in the school
* Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online
* Liaising with relevant members of staff on online safety matters, e.g. the SENDCo and ICT Strategic Group and Reboot
* Ensuring online safety is recognised as part of the school’s safeguarding responsibilities and that a coordinated approach is implemented
* Ensuring safeguarding is considered in the school’s approach to remote learning
* Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure
* Understanding the filtering and monitoring processes in place at the school
* Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school
* Maintaining records of reported online safety concerns as well as the actions taken in response to concerns
* Monitoring online safety incidents to identify trends and any gaps in the school’s provision, and using this data to update the school’s procedures.
* Reporting to the Governing Body about online safety on a half-termly basis.
* Working with the Headteacher and ICT Strategic Group and Reboot to conduct termly light-touch reviews of this policy
* Working with the Headteacher and Governing Body to update this policy on an annual basis

ICT Strategic Group and Reboot will be responsible for:

* Providing technical support in the development and implementation of the school’s online safety policies and procedures
* Implementing appropriate security measures as directed by the Headteacher
* Ensuring that the school’s filtering and monitoring systems are updated as appropriate
* Working with the DSL and Headteacher to conduct termly light-touch reviews of this policy

All staff members will be responsible for:

* Taking responsibility for the security of ICT systems and electronic data they use or have access to
* Modelling good online behaviours
* Maintaining a professional level of conduct in their personal use of technology
* Having an awareness of online safety issues
* Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online
* Reporting concerns in line with the school’s reporting procedure
* Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum

Pupils will be responsible for:

* Adhering to the Technology Acceptable Use Agreement (AUA) (Appendix 2 EY and KS1, Appendix 3 KS2) and other relevant policies
* Seeking help from school staff if they are concerned about something they or a peer have experienced online
* Reporting online safety incidents and concerns in line with the procedures within this policy

# 3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school’s approach to online safety, with support from deputies and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils’ safety online. The DSL should liaise with the police or children’s social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

* Staff and governors receive regular training
* Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
* Online safety is integrated into learning throughout the curriculum
* Assemblies are conducted half-termly on the topic of remaining safe online
* Safer Internet Day is celebrated each year
* Teach Computing units of work
* PSHE lessons
* Online safety displays around school
* Wake up Wednesday posters from National Online Safety are included in the weekly newsletter
* Pupils and staff sign the AUA

**Handling online safety concerns**

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. Confidentiality will not be promised, and information may be shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children’s social care or the police against the victim’s wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children’s social care or the police against the victim’s wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member’s online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Headteacher, it is reported to the Chair of Governors.

Concerns regarding a pupil’s online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and ICT Strategic Group and Reboot, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school’s response are recorded by the DSL and will be recorded on the online safety incident log (Appendix 1).

# 4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

* Threatening, intimidating or upsetting text messages
* Threatening or embarrassing pictures and video clips sent via mobile phone cameras
* Silent or abusive phone calls or using the victim’s phone to harass others, to make them think the victim is responsible
* Threatening or bullying emails, possibly sent using a pseudonym or someone else’s name
* Unpleasant messages sent via instant messaging
* Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
* Abuse between young people in intimate relationships online i.e. teenage relationship abuse
* Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

# 5. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

* Threatening, facilitating or encouraging sexual violence
* Upskirting, i.e. taking a picture underneath a person’s clothing without consent and with the intention of viewing their genitals, breasts or buttocks
* Sexualised online bullying, e.g. sexual jokes or taunts
* Unwanted and unsolicited sexual comments and messages
* Consensual or non-consensual sharing of sexualised imagery
* Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

# 6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

* Being secretive about how they are spending their time online.
* Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
* Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

**Child sexual exploitation (CSE) and child criminal exploitation (CCE)**

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

**Radicalisation**

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay.

# 7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil’s mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

# 8. Online hoaxes and harmful online challenges

For the purposes of this policy, an **“online hoax”** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **“harmful online challenges”** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

* In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
* Careful to avoid needlessly scaring or distressing pupils.
* Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
* Proportional to the actual or perceived risk.
* Helpful to the pupils who are, or are perceived to be, at risk.
* Appropriate for the relevant pupils’ age and developmental stage.
* Supportive.
* In line with the Child Protection and Safeguarding Policy.

Where the DSL’s assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils’ exposure to the risk is considered and mitigated as far as possible.

# 9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

* **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
* **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and ‘booting’, which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil’s use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

# 10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

# 11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

* Relationships and health education taught through PSHE
* Computing

Online safety teaching is always appropriate to pupils’ ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

* How to evaluate what they see online
* How to recognise techniques used for persuasion
* Acceptable and unacceptable online behaviour
* How to identify online risks
* How and when to seek support
* Knowledge and behaviours that are covered in the government’s online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum.

The school’s approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

**Content Risks**

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

**Contact Risks**

The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

**Conduct Risks**

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

**Commerce Risks**

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will be involved with the development of the school’s online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENDCo and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

# 12. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

* Computers
* Laptops
* iPads
* Chrome Books
* Email
* Cameras
* Visualisers

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

**13. Use of electronic devices (including mobile phones)**

Mobile phones, tablets and other personal electronic devices have become widely available and accessible to pupils.

Swain House Primary School accepts that personal mobile phones and tablets are often given to pupils by their parents to ensure their safety and personal security, but understands that such devices pose inherent risks and may jeopardise the learning environment.

As a school, we must strike a balance between personal safety and a suitable educational setting. We understand that parents may wish for their child to carry a mobile phone for their personal safety, whilst pupils may wish to bring additional devices to school for other reasons. This section of the online safety policy establishes how personal electronic devices should be used in school to ensure both personal safety and an appropriate learning environment.

Personal electronic devices include, but are not limited to the following items:

* Mobile phones
* Portable internet devices, e.g. tablets, laptops
* Handheld entertainment systems, e.g. video game consoles

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school’s Technology Acceptable Use Agreement for Pupils.

Staff will use all smart technology in line with the school’s Staff AUA.

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Pupils can loan a Chrome Book if necessary for homework and parents are required to agree and sign the loan agreement, acknowledging the filtering and monitoring used on the devices.

Inappropriate use of smart technology may include:

* Using mobile and smart technology to sexually harass, bully, troll or intimidate peers
* Sharing indecent images, both consensually and non-consensually
* Viewing and sharing pornography and other harmful content

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

# The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

**Staff personal mobile phones**

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, while children are present/during contact time. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staff room). During contact time, staff members who have mobile phones, must keep them in the locked drawer in the classroom or in their personal locker.

There may be circumstances in which it’s appropriate for a member of staff to have use of their phone during contact time. For instance:

* For emergency contact by their child, or their child’s school
* In the case of acutely ill dependents or family members

The Headteacher will decide on a case-by-basis whether to allow for special arrangements. During these times, the mobile phone must be out of sight of children such as in a pocket and be switched to vibrate.

If special arrangements are not deemed necessary, school staff can use the school office number 01274 639 049 as a point of emergency contact.

# Data protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information.

# Safeguarding

Staff must refrain from giving their personal contact details to parents or pupils, including connecting through social media and messaging apps. Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents or pupils. Staff must not contact parents or pupils via social media platforms or through any messaging app. Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil unless it is agreed by the Headteacher.

# Using personal mobile phones for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren’t limited to:

* Emergency evacuations
* Emergency invacuations
* Supervising off-site trips
* Supervising residential visits

In these circumstances, staff will:

* Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
* Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil
* Refrain from using their phones to contact parents unless necessary. If needed, contact can be made via the school office. If a staff member’s own mobile phone is necessary to contact parents, they will block their number so parents cannot obtain it.

# Staff work phones

Some members of staff are provided with a mobile phone by the school for work purposes.

Only authorised staff are permitted to use school phones, and access to the phone must not be provided to anyone without authorisation.

Staff must:

* Only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet
* Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line with our staff code of conduct.

# Sanctions

Staff that fail to adhere to this policy may face disciplinary action.

See the school’s staff disciplinary policy for more information.

# Pupils’ personal mobile phones

Children are allowed to bring a mobile phone into school if parents believe this is necessary from Year 5.

* This might be necessary if children are -
  + Travelling to school by themselves
  + Young carers who need to be contactable

Mobile phones must be handed in at the start of the day and placed in the class box. The box will then go down to the office and be stored until the end of the day

# Sanctions

If a pupil uses their mobile phone during the school day, their mobile phone may be confiscated and placed in the school office class box. It will be returned to a parent at the end of the day and a consequence may be given.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously, and will involve the police or other agencies as appropriate.

Such conduct includes, but is not limited to:

* Sexting (consensual and non-consensual sharing nude or semi-nude images or videos)
* Upskirting
* Threats of violence or assault
* Abusive calls, emails, social media posts or texts directed at someone on the basis of someone’s ethnicity, religious beliefs or sexual orientation

# Use of mobile phones by parents, volunteers and visitors

Parents, visitors and volunteers (including Governors and contractors) must adhere to this section of the online safety policy as it relates to individuals who are on the school site during the school day.

This means:

* Not taking pictures or recordings of pupils, unless it’s a public event (such as a school fair), or of their own child
* Using any photographs or recordings for personal use only, and not posting on social media without consent
* Not using phones in lessons, or when working with pupils

Parents or volunteers supervising school trips or residential visits must not:

* Use their phone to make contact with other parents
* Take photos or recordings of pupils, their work, or anything else which could identify a pupil

# Loss, theft or damage

Pupils bringing phones to school must ensure that phones are switched off when on the school premises. When pupils hand their phone in at the start of the school day, they will be taken, in a class box, and stored securely in the Admin Office. The boxes will be returned to class at the end of the day.

Pupils must secure their phones as much as possible, including using passwords or pin codes to protect access to the phone’s functions. Staff must also secure their personal phones, as well as any work phone provided to them. Failure by staff to do so could result in data breaches.

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

Lost phones should be returned to the main office. The school will then attempt to contact the owner.

# 14. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school’s approach to online safety and their role in protecting their children. A copy of the Acceptable Use Agreement will be shared with parents at the beginning of each academic year and they are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

* Child sexual abuse, including grooming
* Exposure to radicalising content
* Sharing of indecent imagery of pupils, e.g. sexting
* Cyberbullying
* Exposure to age-inappropriate content, e.g. pornography
* Exposure to harmful content, e.g. content that encourages self-destructive behaviour

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

* Parents’ evenings
* Newsletters and other communications home
* Wake up Wednesday posters sent in the weekly newsletter
* West Yorkshire Police information sessions
* School website
* Online resources

# 15. Internet access

Pupils, staff and other members of the school community will only be granted access to the school’s internet network once they have read and signed the Acceptable Use Agreement   
(Appendix 4 for staff and governors).

All members of the school community will be encouraged to use the school’s internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

# 16. Filtering and monitoring online activity

The Governing Body will ensure the school’s ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE’s ‘[Filtering and monitoring standards for schools and colleges](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges)’. The Governing Body will ensure ‘over blocking’ does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school’s safeguarding needs.

The Headteacher, ICT Strategic Group and Reboot will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils’ ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT Strategic Group and Reboot will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Headteacher. Prior to making any changes to the filtering system, ICT Strategic Group and Reboot and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT Strategic Group and Reboot. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT Strategic Group and Reboot, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school’s network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

All staff will receive regular training on the operation and purpose of filtering and monitoring systems, including their role in safeguarding.

Personal devices connected to the school's network will be subject to the same filtering and monitoring standards to ensure consistent safeguarding measures.

Filtering and monitoring systems will undergo at least an annual review to assess their effectiveness and relevance.

# 17. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by Reboot. Firewalls will be switched on at all times. Reboot will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to Headteacher, DSL and Reboot.

All members of staff will have their own unique usernames and private passwords to access the school’s systems. Pupils in KS1 and above will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users will inform a member of the ICT Strategic Group if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

The digital lead (DSL) will be responsible for implementing appropriate network security measures in liaison with the DPO and Headteacher.

# 18. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and the Acceptable Use Agreement.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT Strategic Group and Reboot. The school’s monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. ICT Strategic Group and Reboot will organise an annual assembly where they explain what a phishing email and other malicious emails might look like – this assembly will includes information on the following:

* How to determine whether an email address is legitimate
* The types of address a phishing email could use
* The importance of asking “does the email urge you to act immediately?”
* The importance of checking the spelling and grammar of an email

# 19. Generative artificial intelligence (AI)

When deciding whether to use generative AI, safety will be the top priority. Any use of AI tools by staff and pupils will be carefully considered and assessed, evaluating the benefits and risks of its use in the school.

AI tools will only be used in situations where there are specified clear benefits that outweigh the risks, e.g. where it can reduce teacher workload, and the school will ensure that any use of AI tools comply with wider statutory obligations, including those outlined in KCSIE.

The school will carry out an AI Risk Assessment, which includes plans for mitigating against unauthorised use cases.

Pupils will only be permitted to use generative AI in the school with appropriate safeguards in place, e.g. close supervision and the use of tools with appropriate filtering and monitoring features in place.

For any use of AI, the school will:

* Comply with age restrictions set by AI tools and open access large language models (LLMs).
* Consider online safety, including AI, when creating and implementing the school’s approach to safeguarding and related policies and procedures.
* Consult KCSIE to ensure all statutory safeguarding obligations and AI tools are used safely and appropriately.
* Refer to the DfE’s [generative AI product safety expectations](https://www.gov.uk/government/publications/generative-ai-product-safety-expectations) and [filtering and monitoring standards](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges).

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils’ age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupils’ ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

The school will introduce a comprehensive Safe Use of AI Policy that clearly defines how AI technologies will be utilised responsibly and securely. This policy will outline the potential risks associated with misuse, as well as the safeguarding measures the school will implement to ensure the safe and ethical application of AI tools

# 20. The school website

The Headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

# 21. Remote learning

All remote learning will be delivered in line with the school’s Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

# 22. Monitoring and review

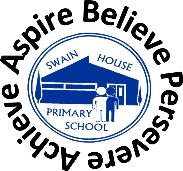
The school recognises that the online world is constantly changing; therefore, the DSL, ICT Strategic Group and Reboot and the Headteacher conduct termly light-touch reviews of this policy to evaluate its effectiveness.

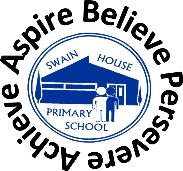
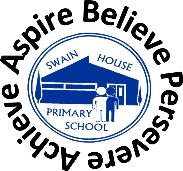
The Governing Body, Headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2026.

Any changes made to this policy are communicated to all members of the school community

**Appendix 1 - Online Safety Incident Report Log**

**Appendix 2 - Acceptable Use Agreement for EYs and KS1**

**Device and technology acceptable use agreement for pupils in EY and KS1**

We know that using technology is an important part of your learning experience. We want everyone to be able to use technology safely.

This agreement sets out the rules around using technology at school.

When I use a device and get on the internet in school, I will

* Only use websites that a teacher has told me to
* Be kind to others online
* Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
* Only use the username and password I have been given
* Never share my password with anyone
* Never give my personal information (my name, address or telephone numbers) to anyone
* Check with my teacher before I print anything
* Log off or shut down a computer when I have finished using it
* Tell my teacher if I see anything that upsets me or my friends. I will close the lid

I understand that the school will monitor the websites I visit and that there will be consequences if I don’t follow the rules

Signed – \_\_\_\_\_\_\_\_\_\_\_\_\_ class

**Appendix 3 - Acceptable Use Agreement for KS2**

**Device and technology acceptable use agreement for pupils in KS2**

At Swain House Primary School, we know that using technology is an important part of your learning experience. We want everyone to be able to use technology safely.

This agreement will set out the rules around using technology and devices.

I understand school will monitor what I am looking at online and will filter websites that may be inappropriate for me to look at. I understand that failure to follow the AUP will lead to consequences in line with the Behaviour Policy.

**Personal and device security**

I will:

* keep my information safe
* keep my password private and not share personal information about myself with someone online
* only access websites and apps that I have been given permission to use
* tell a known adult immediately if I find any material which might upset, distress or harm me of others
* log off or shutdown a device when I have finished working on it
* only search for what I have been asked to
* only use the email account that has been set up for me by the school
* only open emails from people I know

**School-owned devices**

I will:

* only use school-owned devices at school
* take care of school-owned devices when I am using them
* tell a member of staff if a school-owned device is damaged or lost when I am using it
* tell a member of staff if I think something has happened in relation to the security of the device
* not send any inappropriate emails or messages
* not access any social media sites

**Mobile phones**

I understand that if my personal devices are lost, damaged or stolen, it is not up to the school to pay for any costs

I will:

* ensure I put my mobile phone into the class box when I arrive in school and ensure it is switched off
* not use my mobile phone to send inappropriate messages, images, videos or other content
* not use my personal devices to view, store, download or share any inappropriate, harmful or illegal content
* not bring my mobile phone to any school disco

**Social media**

I will:

* think about what I post about the school on social media and make sure I do not post anything that could be harmful to any member of the school community
* not send ‘friend’ or ‘follow’ requests to members of staff on social media
* not send any abusive, threatening or otherwise inappropriate messages on social media
* not arrange to meet anyone offline

**Signed by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ class**

**Appendix 4 - Acceptable Use Agreement for staff and governors**

**Device and technology acceptable use agreement for staff and governors**

I will:

* Only use the approved email accounts that have been provided to me when sending communications regarding school business
* Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected

**School-owned devices**

I will:

* Understand that the usage of my school-owned devices will be monitored
* Transport school-owned devices safely
* Provide suitable care for my school-owned devices at all times
* Only communicate with pupils and parents on school-owned devices using appropriate channels
* Ensure I install and update security software on school-owned devices as directed by Reboot
* Seek permission from the Headteacher before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors
* Immediately report any damage or loss of my school-owned devices to the ICT Strategic Team
* Immediately report any security issues, such as downloading a virus, to the ICT Strategic Team
* Make arrangements to return school-owned devices to the ICT Strategic Team upon the end of my employment at the school

I will not:

* Not permit any other individual to use my school-owned devices, unless otherwise agreed by the Headteacher
* Install any software onto school-owned devices unless instructed to do so by the Headteacher or Reboot
* Use school-owned devices to send inappropriate messages, images, videos or other content
* Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content
* Use school-owned devices to access personal social media accounts
* Share my password with others or log into the school’s network using someone else’s details

**Personal devices**

I will:

* Only use personal devices during out-of-school hours, including break and lunch times unless I have permission from the Headteacher
* Ensure personal devices are either switched off or set to silent mode during school hours
* Only make or receive calls in specific areas, e.g. the staff room
* Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom
* Understand that I am liable for any loss, theft or damage to my personal devices

**Social media and online professionalism**

I will:

* Understand that I am representing the school and behave appropriately when posting on school social media accounts
* Ensure I apply necessary privacy settings to social media accounts
* Not post anything on social media during my working hours
* Not post of social media when I am working from home during my working hours

I will not:

* Communicate with pupils over personal social media accounts
* Accept ‘friend’ or ‘follow’ requests from any pupils over personal social media accounts
* Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school’s reputability
* Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website
* Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos
* Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels

**Working from home**

I will:

* Ensure I obtain permission from the Headteacher and DPO before any personal data is transferred from a school-owned device to a personal device
* Ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised
* Ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted
* Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working

**Reporting misuse**

I will:

* Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the Headteacher
* Understand that my use of the internet will be monitored by the ICT Strategic Group and recognise the consequences if I breach the terms of this agreement
* Understand that the Headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement

**Agreement**

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

|  |  |
| --- | --- |
| **Name** |  |
| **Signature** |  |
| **Date** |  |