

ST JOHN THE BAPTIST C OF E PRIMARY SCHOOL



Life in all its fullness

Online Safety and Acceptable Use Policy

September 2023

- A happy, healthy, safe place to learn how to look after our bodies and minds
 - A place to learn 'People Skills' to prepare us to be good citizens.

Online Safety and Acceptable Use Policy

Introduction

We will endeavour to keep our pupils safe while using technology and online services and install the school Christian values of wisdom, self discipline and humility. We understand 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, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **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:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- People Skills Policy (RSE policy)
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidential Reporting and Whistleblowing Policy
- Data Retention Policy
- Child on Child Abuse Policy
- Computing policy

2. Roles and responsibilities

The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- 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.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is 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 and safeguarding.
- Supporting the DSL (if not the headteacher) and the deputy 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.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- 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 governing body to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- 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 SENCO and ICT technician.
- 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.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.

- Ensuring all members of the school community understand the reporting procedure.
- 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.
- Working with the headteacher and governing body to update this policy on an annual basis.

The ICT technician is 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 and work efficiently.

All staff members are 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 are responsible for:

- Adhering to the Acceptable Use Agreement 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 importance of online safety is integrated across all school operations in the following ways:

- Staff 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 e.g. through the computing and People Skills curriculums
- Assemblies/Collective Worship are conducted on the topic of remaining safe online during Safer Internet day

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.

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, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. 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 technician, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection 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 Policy.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyberbullying

Cyberbullying can include 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
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging

- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

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 and 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

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 responds 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 are reported to the DSL, who will investigate the matter in line with the Child-on-Child Abuse Policy and the Child Protection Policy. Please see these policies for further information.

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, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.

- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- 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.
- 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 Guidance. 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, who will handle the situation in line with the Prevent Duty.

7. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

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 school's Pupils Health and Wellbeing 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 Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, 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 even to individual children 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. Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. 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.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, the Child-on-Child Abuse Policy and the Child Protection Policy.

10. Online safety and the curriculum

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

- People Skills (PSHE including RSE)
- Computing

Teaching is always appropriate to pupils' ages and developmental stages. A planned online safety curriculum is provided as part of the Computing scheme of work for computing lessons and is prioritised annually for all classes. Appropriate differentiation is in place to ensure the safety of more vulnerable children (for example those with SEND or LAC).

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 (both in Computing and People Skills) include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix A of this policy.

The DSL is 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.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils 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 review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher or DSL 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 considers 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 advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are 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 ensures 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 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 Policy.

11. Use of technology in the classroom

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

- Laptops
- Tablets
- Internet
- Cameras

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 always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

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

12. Use of smart technology

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 pupil rules (Appendix D).

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the pupil rules (Appendix D).

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.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the school.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

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 SMART rules (Safe, Meeting, Accepting, Reliable, Tell) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

13. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Parent Carer Consent Form and online safety rules at the beginning of each academic year and 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 is raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources including the school's website

14. Internet access

Staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

All members of the school community are 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.

15. Filtering and monitoring online activity

The governing body ensures the school's ICT network has appropriate filters and monitoring systems in place. The governing body ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The headteacher and ICT technician undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are 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. The ICT technician undertakes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the headteacher. Reports of inappropriate websites or materials are made to the ICT technician immediately, who investigates the matter and makes any necessary changes.

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

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

16. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the ICT technician. Firewalls are switched on at all times. The ICT technician reviews the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to the ICT technician.

All members of staff have their own unique usernames and private passwords to access the school's systems. Staff members and pupils are responsible for keeping their passwords private. Passwords should have a minimum and maximum length appropriate for the relevant website and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users inform the ICT technician if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time (a 'supply' laptop is available for use by supply teachers and will be monitored through a sign in sheet system). If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

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

17. Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Confidential and Whistleblowing Policy.

Staff are given approved school email accounts and are only 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 must agree to and sign the Acceptable Use Agreement. Personal email accounts are not permitted to be used for school use. Any email that contains sensitive or personal information will be anonymised or sent using secure and encrypted email if not using school email systems.

Staff members and pupils are required to block spam and junk mail and report the matter to the ICT technician. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened. Microsoft Teams is our main method of communication.

Any cyber-attacks initiated through emails are managed in line with the Data and Cyber-security Breach Prevention and Management Plan.

18. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff are not permitted to use social media for personal use during lesson time. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL and headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

19. The school website

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

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the provisions in the Use of Children’s Images Policy are met.

20. Use of devices

School-owned devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school’s Acceptable Use Policy for staff, governors and visitors (see Appendix C) and the Staff Code of Conduct.

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

School-owned devices are used in accordance with the Acceptable Use Policy (Appendix C) for staff, and the Internet Safety Rules for Pupils (Appendix D) as applicable. All school-owned devices are password protected.

The ICT technician reviews all school-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material or malware on the devices.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

Personal devices

Any personal electronic device that is brought into school is the responsibility of the user.

Personal devices are not permitted to be used in the following locations:

- Toilets
- Rooms in which children are getting changed

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

Pupils are not permitted to use their personal devices during lesson time or when moving between lessons. If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

21. Remote learning

All remote learning is delivered in line with the school's Remote Learning Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

22. Monitoring and review

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

The governing body, headteacher and DSL 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 2024.

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

Appendices

- Online harms and risks – curriculum coverage
- Parents/carers consent form and online safety rules
- Staff, governor and visitor acceptable use policy
- Use of digital images
- Online safety rules for KS1 and KS2

Appendix A: Online harms and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following:</p> <ul style="list-style-type: none"> ● That age verification exists and why some online platforms ask users to verify their age ● Why age restrictions exist ● That content that requires age verification can be damaging to under-age consumers ● What the age of digital consent is (13 for most platforms) and why it is important 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> ● Health education ● Computing
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online. Teaching includes the following:</p> <ul style="list-style-type: none"> ● What a digital footprint is, how it develops and how it can affect pupils' futures ● How cookies work ● How content can be shared, tagged and traced ● How difficult it is to remove something once it has been shared online ● What is illegal online, e.g. youth-produced sexual imagery (sexting) 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> ● People Skills ● Computing
Disinformation, misinformation and hoaxes	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following:</p>	<p>This risk or harm is covered in the following curriculum areas:</p>

	<ul style="list-style-type: none"> • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Malinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true 	<ul style="list-style-type: none"> • People Skills • Computing
<p>Fake websites and scam emails</p>	<p>Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following:</p> <ul style="list-style-type: none"> • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
<p>Online fraud</p>	<p>Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following:</p> <ul style="list-style-type: none"> • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing

	<ul style="list-style-type: none"> • What ‘good’ companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts 	
Password phishing	<p>Password phishing is the process by which people try to find out individuals’ passwords so they can access protected content. Teaching includes the following:</p> <ul style="list-style-type: none"> • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
Personal data	<p>Online platforms and search engines gather personal data – this is often referred to as ‘harvesting’ or ‘farming’. Teaching includes the following:</p> <ul style="list-style-type: none"> • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
Persuasive design	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following:</p> <ul style="list-style-type: none"> • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
Privacy settings	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following:</p> <ul style="list-style-type: none"> • How to find information about privacy settings on various sites, apps, devices and platforms 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills

	<ul style="list-style-type: none"> • That privacy settings have limitations 	<ul style="list-style-type: none"> • Computing
Targeting of online content	<p>Much of the information seen online is a result of some form of targeting. Teaching includes the following:</p> <ul style="list-style-type: none"> • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
How to stay safe online		
Online abuse	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following:</p> <ul style="list-style-type: none"> • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
Challenges	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following:</p> <ul style="list-style-type: none"> • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills
Fake profiles	<p>Not everyone online is who they say they are. Teaching includes the following:</p>	<p>This risk or harm is covered in the</p>

	<ul style="list-style-type: none"> • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles 	<p>following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
Grooming	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following:</p> <ul style="list-style-type: none"> • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police <p>At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.</p>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills
Unsafe communication	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following:</p> <ul style="list-style-type: none"> • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
Wellbeing		
Impact on confidence (including body confidence)	<p>Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following:</p> <ul style="list-style-type: none"> • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers 	<p>This risk or harm is covered in the following curriculum areas:</p>

	<ul style="list-style-type: none"> • That ‘easy money’ lifestyles and offers may be too good to be true • The issue of photo manipulation, including why people do it and how to look out for it 	<ul style="list-style-type: none"> • People Skills
Impact on quality of life, physical and mental health and relationships	<p>Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following:</p> <ul style="list-style-type: none"> • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills
Online vs. offline behaviours	<p>People can often behave differently online to how they would act face to face. Teaching includes the following:</p> <ul style="list-style-type: none"> • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
Reputational damage	<p>What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following:</p> <ul style="list-style-type: none"> • Strategies for positive use • How to build a professional online profile 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • People Skills • Computing
Suicide, self-harm and	<p>Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should</p>	<p>Addressed when raised by pupils.</p>

eating disorders	take care to avoid giving instructions or methods and avoid using language, videos and images.	
------------------	--	--



Appendix B - Parent/Carers consent form and online safety rules

All pupils will have access to the school's computer facilities including the internet as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the online safety rules have been understood and agreed.

Pupils Name: _____

Parent/Carer Name: _____

- As the parent or legal guardian of the above pupil, I have read and understood the attached school rules and now grant permission for my son/daughter to use the internet, school learning platform (Teams) and other IT facilities at School.
- I know that my son/daughter has signed an online safety agreement and they have a copy of the school online safety rules.
- We have discussed this document and they agree to follow the rules to support the safe and responsible use of IT at School.
- I accept that the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that they will take every reasonable precaution to keep pupils safe and to prevent pupils accessing inappropriate materials.
- The school has an educationally filtered service, restricted access email and provides age appropriate teaching around internet use and online safety issues.
- I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parents Signature: _____ Date: _____

Please complete and return to the school office.



Appendix C - Staff, Governors and Visitor Acceptable Use Policy/IT Code of Conduct

IT and the related technologies such as email, the internet and mobile devices are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents.

- I appreciate that IT includes a wide range of systems and devices including mobile phones, PDAs, digital cameras, email, social networking and may include personal IT devices when used for school business.
- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activities carried out under my user name.
- I will only use the school email, internet, learning platform or any related technologies for professional purposes.
- I will ensure that personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the head teacher or governing body.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without permission.
- I will ensure that my online activity both in school and outside school will not bring my professional role into disrepute.
- I will ensure that all electronic communications with parents, pupils and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's e-safety policy and help pupils to be safe.
- I will report any incidents of concern regarding children's safety to the e-safety coordinator, the Designated Person or their assistant.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

User Signature

I agree to follow the code of conduct and support the safe use of IT throughout the school

Full Name: _____

Job Title: _____

Signature _____ Date _____

Appendix D – Online Safety Rules for Key Stage 1

Think then Click



I only use the internet when an adult has given me permission.

I am kind on the internet and tell an adult if someone isn't kind to me.



I will tell an adult if someone tries to talk or message me in an app or on the internet.

I can search within websites chosen by an adult.



I always ask an adult if I get lost on an app or website, or if something unexpected pops up.

I never tell anyone my name, age, school or where I live on the internet.



Online Safety Rules for Key Stage 2

Think then Click

- I will follow the SMART rules:
 - I will stay SAFE by never give out my name, passwords or personal information online.
 - I will never arrange to MEET anyone new that I have only chatted with on-line.
 - I will not ACCEPT e-mails, or open pop-ups or messages, sent by someone I don't know.
 - I will question how RELIABLE information online is.
 - If I'm not sure, or I see something that upsets me, I will TELL a responsible adult.
- I only use the internet if I have permission.
- I will only use websites or apps that an adult has chosen.
- I will use safe search engines for research.
- I will be polite and friendly when communicating with people online.
- I will seek permission from a responsible adult before posting an image or video of myself



Name: _____

Signed: _____

Date: _____