Online Safety Policy

Whole School

Contents

Statement of intent

Great Bridge 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, 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 (2021) 'Keeping children safe in education 2021'
- 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 (2019) 'Teaching online safety in school'
- DfE (2018) '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
- RSE and Health Education Policy
- Staff Code of Conduct
- Behavioural Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Photography Policy
- Prevent Duty Policy
- Pupil Remote Learning Policy
- Technology Acceptable Use Agreement for Pupils (See Appendices A & B)
- Technology Acceptable Use Agreement – Staff (See Appendix C)

2. Roles and responsibilities

The governing board 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, teacher training and safeguarding.
- Supporting the DSL 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.
- 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 board to update this policy on an annual basis.

The DSL and deputy DSL's are 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 technicians.
- 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.
- 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 board about online safety incidents on a termly basis using CPOMs to run a report.
- Working with the headteacher and governing board to update this policy on an annual basis.

The Computing Lead Teacher is responsible for:

- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.

- Working with the headteacher and ICT technicians to update this policy on an annual basis.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Working with the SMSC Lead Teacher to ensure parity between what is taught as part of Relationships Education.

ICT technicians are responsible for:

(The school employs third party external support – SIPS, who are responsible in conjunction with the in-school junior technician)

- 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 reviewed regularly to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact while online at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Conducting a full security check on a monthly basis.

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 using CPOMS in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Parents are responsible for:

- Notifying a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensuring their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

Healthy relationships – Disrespect Nobody

Parental guides to keeping children safe online - Skips Safety Net

CEOP to report online safety concerns - https://www.ceop.police.uk/safety-centre/

Online Safety for Children - Tips & Guides | NSPCC

Parental controls offered by your home internet provider | Safer Internet Centre

10 Internet Safety Tips - Staying Safe Online | SWGfL

Staying safe online | Childline

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement (See appendices A and B) 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 safeguarding training which includes online safety updates
- Staff receive 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 termly on the topic of remaining safe online
- Keeping safe online is discussed at least annually at school council meetings
- Guidance for parents is available on the school website, in newsletters and they are invited to an annual webinar (or similar session).

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, Whistleblowing 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 technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural 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 on CPOMs and are reported to Governors in the HT report.

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. Peer-on-peer 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 peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with 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, 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 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, who will handle the situation in line with the Prevent Duty Policy.

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 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, 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. 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, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

10. 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 Child Protection and Safeguarding Policy.

11. Online safety and the curriculum

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

- PSHE / RSE
- 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
- 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
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online 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 D 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 and 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 and DSL 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 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 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 is used during lessons, including the following:

- Computers
- Laptops / Chromebooks
- Tablets
- Email
- Cameras
- Lego WeDo
- Beebots and other programmable devices

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.

13. 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 school's Technology Acceptable Use Agreement for Pupils (Appendices A & B).

Staff will use all smart technology and personal technology in line with the school's Online Safety Policy and Technology Acceptable Use Agreement for Staff (Appendix C)

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 school's acceptable use of ICT agreement for pupils.

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 during the school day.

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 4C's (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.

14. 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 Acceptable Use Agreement at the beginning of each key stage 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 via the availability of this policy 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 - 1:1 discussions with parents as needed

- Parental training sessions – delivered annually by Skips Educational
- Termly Newsletters
- Online resources with links on website

15. Internet access

Pupils, 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. A record is kept of users who have signed this Acceptable Use Agreement (Appendix C) in the school office.

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.

16. Filtering and monitoring online activity

The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place. These are currently provided by LGfL and self-certified to the UK Safer Internet Centre. The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

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. Global changes to the filtering system are made by LGfL as necessary and ICT technicians ensure the server is up to date to include all LGfL filtering and monitoring updates so that the systems are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment. Any changes made to the system are recorded by ICT technicians. Reports of inappropriate websites or materials are made to an 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 technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behavioural 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 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 and Safeguarding Policy.

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times. ICT technicians review 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 ICT technicians.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils in key stage 2 are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords do not expire in line with DPO guidance but must be changed in the event of a data breach.

Users inform ICT technicians if they forget their login details, who will reset their password so that they can regain access. Users are not permitted to share their login details with unauthorised persons and are not allowed to log in as another user without their explicit permission. If a user is found to be 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.

18. Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement, and Staff code of conduct and Volunteer Confidentiality Policy.

Staff and pupils (when necessary) 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 and pupils must agree to and sign the Acceptable Use Agreement. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians. 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.

Any cyber-attacks are reported to LGfL, via SIPS and are handled on a global level. If a particular email has been sent to their sites, they will act on them in the best process for that particular attack.

19. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff and pupils can use personal social media during break and lunchtimes; however, inappropriate or excessive use of

personal social media during school hours may result in the removal of internet access or further action. 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 receive training on how to use social media safely and responsibly. 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 Behavioural Policy.

Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

20. 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 Photography Policy are met.

21. Use of devices

School-owned devices

Staff members may use the following devices to assist with their work:

- Laptop
- Tablet

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons. In – school use is monitored and supervised by teachers and school staff in line with the Technology Acceptable Use Agreement for pupils (Appendices A and B).

Parents of pupils who need to loan school-owned devices must sign an agreement before this loan takes place to take responsibility for supervision / monitoring of the use of these devices at home. These devices will have Home Protect software installed and Safari or other internet browsers disabled to ensure safe access to the internet

School-owned devices are used in accordance with the Technology Acceptable Use Agreement. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

ICT technicians review 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. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

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

Personal devices are used in accordance with the Technology Acceptable Use Agreements (Appendices A, B & C). Any personal electronic device that is brought into school is the responsibility of the user.

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, including on off-site visits.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Whistleblowing 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 the school day. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use. Year 6 who have permission to walk home may bring a personal mobile phone into school and will turn it off before entering the school building. They will hand it in to the designated staff member at the start of the school day, for safe-keeping. This will be returned to them at the end of the school day.

Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Pupils' devices can be searched, screened and confiscated if a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

22. Remote learning

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.

23. Monitoring and review

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

The governing board, 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 **January 2023**.

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

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

At Great Bridge, we know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

I will:

- ✓ Only use technology, such as a computer or iPad, when a teacher has given me permission.
- ✓ Only use technology for the reason I have been asked to use it.
- ✓ Only use the internet when a teacher has given me permission.
- ✓ Ask for help when I have a problem using the technology.
- ✓ Look after the device and try not to damage it.
- ✓ Tell the teacher if my device is not working or damaged.
- ✓ Tell the teacher if I think someone else is not using technology safely or correctly.
- ✓ Tell the teacher if I see something online that I think is inappropriate or that makes me upset.

I will not:

- ✘ Tell another pupil my username and password.
- ✘ Share personal information, such as my age and where I live, about myself or my friends online.
- ✘ Access social media, such as Facebook and WhatsApp.
- ✘ Speak to strangers on the internet.
- ✘ Take photos of myself or my friends using a school device.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Please read each statement and provide a tick to show that you agree, and then write your name below.

- ☐ I understand why it is important to use technology safely and correctly.
- ☐ I understand my responsibilities when using technology.
- ☐ I understand that I may not be allowed to use technology if I do not use it safely and correctly.
- ☐ I will follow these rules at all times.

Pupil Name (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
At Great Bridge, we know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them. **I will read and follow the rules in the acceptable use agreement policy** **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** 1. Always use the school's ICT systems and the internet responsibly and for educational purposes only 2. Only use them when a teacher is present, or with a teacher's permission 3. Keep my username and passwords safe and not share these with others 4. Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer 5. Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others 6. Always log off or shut down a computer when I'm finished working on it **I will not:** 7. Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity 8. Open any attachments in emails, or follow any links in emails, without first checking with a teacher 9. Use any inappropriate language when communicating online, including in emails or on Class DoJo 10. Log in to the school's network using someone else's details 11. Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **Year 6 only: If I bring a personal mobile phone or other personal electronic device into school:** 12. I will turn it off before I enter the school building. 13. I will hand it in to my class teacher at the start of the school day, for safe-keeping. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.** **Please read each statement and provide a tick to show that you agree, and then write your name below.** ☐ I understand why it is important to use technology safely and correctly. ☐ I understand my responsibilities when using technology. ☐ I understand that I may not be allowed to use technology if I do not use it safely and correctly. ☐ I will follow these rules at all times.	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Technology acceptable use agreement for staff

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the **headteacher** in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, on or off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. Using technology in school

- I will only use ICT systems which have been permitted for my use by the **headteacher**, such as:
  - Computers.
  - Laptops.
  - Tablets.
- I will only use the approved email accounts that have been provided to me for school purposes.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any other staff, pupils or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the UK GDPR.
- **I will lock access to devices and systems when they are not in use.**
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing teaching materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the computing lead teacher, ICT technicians or headteacher.
- I will only use recommended removable media and will keep this securely stored in line with the UK GDPR.
- I will only store data on removable media or other technological devices that have been encrypted or pseudonymised.
- I will only store sensitive personal data where it is absolutely necessary and has been encrypted.
- I will give removable media to the ICT Technicians for safe disposal once I am finished with it.

2. Mobile devices

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that personal mobile devices are either set to silent mode or switched off during school hours, and will only make or receive calls in private.
- I will ensure personal mobile devices are stored in a lockable cupboard/drawer, at my own risk, located in the staffroom or classroom during lesson times.

- **I will not use personal mobile devices to take photographs or videos of pupils or staff, including on off-site visits.**
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices unless permission has been given by the headteacher or computing lead teacher.
- I will not use personal or school-owned mobile devices to communicate with pupils or parents other than through authorized channels such as Class DoJo, work-based emails or by withholding number.
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymised, and give permission for the ICT technicians to erase and wipe data off my device if it is lost or as part of exit procedures.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on a school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the headteacher before accessing the site.
- I will not communicate with pupils or parents over personal social networking sites without disclosing this to the headteacher.
- I will not accept 'friend requests' or 'follow requests' from any pupils or parents over personal social networking sites.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will not 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.

4. Working from home

- I will adhere to the principles of the UK GDPR when working from home.
- I will ensure I obtain permission from the headteacher or school business manager before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.

- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- The school business manager will ensure that staff who will be working from home using personal devices complete annual GDPR training.
- I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.
- I will act in accordance with the school's Online Safety and Data Protection Policies when transporting school equipment and data.

5. Training

- I will ensure I participate in any online safety training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the computing lead teacher and school business manager to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

6. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher.
- I understand that my use of the internet will be monitored by the ICT Technicians and shared with the headteacher if necessary and recognise the consequences if I breach the terms of this agreement.
- I 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.

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

Signed (staff member): Date:

Print name:

Signed (**headteacher**): Date:

Print name:

Appendix D: Online safety – curriculum coverage

Great Bridge uses lesson plans from Switched on Online Safety by Rising Stars to ensure full curriculum coverage of Online Safety. Below is a break down by year group of the key teaching content. This content is also available for parents on our school website.

Year One E-Safety Overview

Unit 1.1 – We are Year 1 rule writers

Creating rules that help us stay safe online

Children help to develop a simple set of age appropriate rules to establish a working framework for online safety for school and home during Year 1.

Online safety focus:

· understand that rules help us stay safe, both in the real world and online.

· suggest strategies for staying safe in different online scenarios.

· help to develop a set of online safety rules that are easily understood and appropriate for Year 1.

Unit 1.2 – We are kind and thoughtful

Understanding the impact of our behaviour on others

Children carry out an experiment with two apples to see the impact of unkind behaviour.

Online safety focus:

· understand that unkind behaviour online can affect other people, even though we can't see them.

· understand that the rules created in Unit 1.1 can be applied to any concerns they may have about their online activities.

Unit 1.3 – We are responsible internet and device users

Remembering to take time out from technology

Children consider how much time they spend using devices and come up with ideas for other activities that they might do instead.

Online safety focus:

· learn the very basic principles of what the internet is.

· understand how people use the internet.

· understand that using computer devices too often can be bad for us and we should take time out form technology to do other things.

· discuss what to do if they see or hear something online that upsets them.

Unit 1.4 – We are information protectors

Understanding what is meant by personal information

Children will find out what is meant by 'personal information' and how this should always be kept private.

Online safety focus:

· understand what is meant by ‘personal information’.

· recognise that anyone online who we don’t know in real life is a stranger.

· understand how we can protect our personal information, including reporting worries to trusted adults.

Unit 1.5 – We are good digital citizens

Finding out what it means to be a good digital citizen

Children find out what is meant by ‘digital citizen’ and develop an awareness that good digital citizenship is important wherever technology is used.

Online safety focus:

· understand what is meant by ‘digital citizen’.

· understand how to be responsible, respectful and safe online.

· understand that being a good digital citizen means having a kind heart, a warning tummy and a thinking brain; all things that keep us safe online.

· recall what to do if something happens online that makes them feel uncomfortable – building on Unit 1.4 – We are information protectors lesson.

Unit 1.6 – We are responsible gamers

Learning how to stay safe when playing online games

Children learn the importance of gaming in a shared space and of taking breaks from gaming.

Online safety focus:

· understand the importance of playing games in shared spaces where grown-ups are available for support.

· understand the importance of taking breaks away from technology.

Year Two E-Safety Overview

Unit 2.1 – We are Year 2 rule writers

Reviewing and editing our online safety guidelines

Children review different online safety scenarios and decide how to respond to these. They then review, discuss and edit the online safety rules they created in Year 1.

Online safety focus:

• consider online safety scenarios encountered in Year 1 (both at school and at home) and appreciate how these new experiences can be used to update their online safety rules.

• consider what strategies they might use if their usual trusted adult is not available

• review and edit their online safety guidelines.

• develop their online safety rules so they are easily understood and appropriate for Year 2 pupils.

Unit 2.2 – We are not online bullies

Creating a strong message against online bullying

Children learn about the consequences of online bullying and the role of a bystander in online bullying situations. They create an anti-online bullying slogan to send a strong message that bullying is never acceptable.

Online safety focus:

• begin to understand the concept of online bullying and the role of the bystander.

• develop an understanding of the consequences of online bullying.

recall their online safety rules for reporting concerns and inappropriate behaviour.

Unit 2.3 – We are safe searchers

Learning how to use search engines safely

Children find out how to use technology safely to find information online. They then will create a 'top tips' list for safe searching.

Online safety focus:

• understand the very basic principles of how search engines work.

• understand the key steps for searching the web safely.

understand how to report concerns when searching the web.

Unit 2.4 – We are code masters

Generating strong passwords and keeping them safe

Children learn that passwords help us to keep information safe. They will then look at the rules for creating a strong password and use these rules to practise generating their own passwords.

Online safety focus:

· understand that passwords are an important part of keeping information safe.

· understand the differences between strong and weak passwords.

understand that sharing a password makes it weak.

Unit 2.5 – We are online behaviour experts

Solving online safety problems

Children watch three short video clips and discuss how the people in them can be better digital citizens. They then develop their own responses to these scenarios through role-play.

Online safety focus:

· understand that the way technology is used is as important as good online behaviour.

· understand that the way we use technology impacts the people around us.

· further develop responses to incidents of poor behaviour online.

Unit 2.6 – We are game raters

Understanding and applying the PEGI rating system for games

Children learn that not all digital games are suitable for everyone. They find out about the PEGI rating system and develop a rating for a game of their choosing.

Online safety focus:

· recognise the PEGI age rating system for digital games.

· understand that the system is useful for helping people decide which games are appropriate.

· understand what to do if someone nearby is playing a game which is inappropriate for them.

Year Three E-Safety Overview

Unit 3.1 – We are Year 3 rule writers

Reviewing and editing our online safety rules

Children review, discuss and edit the online safety rules they created in Year 2. Children then recall their learning from the previous year's online safety lessons and then review different online safety scenarios to decide the best responses to online safety incidents.

Online safety focus:

· Consider online safety scenarios encountered in Year 2 (both at school and at home) and appreciate how these new experiences can be used to refine their online safety rules.

· Consider what new strategies they can apply to online safety scenarios, such as calling Childline.

· Review and edit their online safety guidelines.

· Develop and edit their online safety rules so they are easily understood and appropriate for Year 3 pupils.

Unit 3.2 – We are digital friends

Developing an awareness of online bullying

Children watch a series of short clips around online bullying and examine the role of each person involved. They then discuss the consequences of the action on the victim and perpetrator. Finally, they will review anti-bullying slogans.

Online safety focus:

· begin to understand that information shared online cannot always be controlled

· develop a deeper. understanding of the consequences of online bullying.

· understand the role of a bystander in online bullying.

Unit 3.3 – We are internet detectives

Assessing the trustworthiness of websites

Children will understand that not everything on the internet is true.

They will learn how to decide if a website is trustworthy and develop a checklist of these clues to critically compare a trustworthy and untrustworthy website from a given selection. Finally, they will apply their understanding when discussing this skill with parents at home.

Online safety focus:

· use clues to make choices about which web pages they consider most useful and trustworthy.

· understand that not all links are safe or trustworthy.

· understand different ways to report concerns and inappropriate behaviour.

Unit 3.4 – We are aware of our digital footprint

Understanding the digital trails we leave behind

Children learn what is meant by 'digital footprint' and that everything shared on the internet can be found, shared, broadcast and copied and that it lasts forever. They start to build a picture of their own digital footprint that can be shared with grown-ups at home.

Online safety focus:

· Understand that every time we use the internet we leave a digital trail that can be found, copied, shared and broadcast

· Understand that the things we upload onto the internet last forever.

Unit 3.5 – We are netiquette experts

Practising good netiquette

Children find out what is meant by netiquette and why it is important. They compare and contrast different styles of written communication and help compose a class response to an email and then create a netiquette guide to help promote good online behaviour.

Online safety focus:

· understand that good online behaviour is important for making the internet an enjoyable place for everyone

· understand that email is a widely used form of digital communication that lasts forever and can be shared.

Unit 3.6 – We are avatar creators

Who do we really know online?

Children discover that online identities may be misleading or false. They create their own online avatar, and distribute these randomly and try to guess the identity of each creator.

Online safety focus:

· understand that internet identities are actively constructed by the user

· recognise that internet identities can be misleading or not representative of the creator

· recall that personal information should not be shared by anyone online who we don't know in real life

Year Four E-Safety Overview

Unit 4.1 – We are Year 4 rule writers

Reviewing and editing our online safety rules.

Children recall their learning from the previous year's online safety lessons and then review different online safety scenarios and decide the best response to these. They then review, discuss and edit the online safety rules they created in Year 3.

Online safety focus:

• Consider online safety scenarios encountered in Year 3 (both at school and at home) and appreciate how these new experiences can be used to update their online safety rules.

• Consider what new strategies they can apply to online safety scenarios, beyond talking to a trusted adult.

• Review and edit their online safety guidelines.

• Develop their online safety rules so they are easily understood and appropriate for Year 4 pupils.

Unit 4.2 – We are standing up to peer pressure

Dealing positively with peer pressure

Children find out that access to the internet is not the same among all people and that peer pressure can be both positive and negative. They will scrutinise and discuss a short online safety scenario and decide how to resolve a problem where access to the internet is not the same between two friends.

Online safety focus:

• Understand that peer pressure can be a positive and negative influence.

• Understand that access to the internet is not the same for everyone.

• Recall ways to report concerns and inappropriate behaviour.

Unit 4.3 – We are aware that our online content lasts forever

Getting the message: pre- and post-internet

Children compare and contrast the ways messages were sent before and after the advent of the internet. They then think about a digital medium through which they can spread information as if it was the 1940s, assessing the speed and reach of the message if it was sent via social media today.

Online safety focus:

· Understand that because of the internet, information can be spread more quickly and reach more people now than at any time in the past.

· Understand that although information posted on the internet might not always be true or accurate, it lasts forever.

Unit 4.4 – We are online risk managers

Understanding risk and prevention of information loss

Children learn that hacking can be a criminal activity and clicking on links in suspicious websites or emails can introduce viruses to devices, putting personal information at risk and

stopping the device from working. They will learn ways to protect their devices and accounts and use this information to create a family protection plan to share at home.

Online safety focus:

· Understand the risks involved in clicking on and opening links on suspicious websites and in emails.

· Understand that hacking can be illegal and has consequences for the hacker.

· Develop awareness of viruses and what to do if they think their account has been compromised.

Unit 4.5 – We are respectful of digital rights and responsibilities

Understanding and respecting digital rights and responsibilities

Children discuss three articles from Unicef's Rights of the Child and apply them to digital citizenship, looking at rights and responsibilities as well as consequences of knowingly ignoring responsibilities. They apply these to their own experiences and share a developed digital citizen with their families.

Online safety focus:

· Understand that both digital rights and responsibilities are important to ensure the internet is a great place for everyone.

· Understand that there are consequences for knowingly ignoring rights.

· Further develop a positive and responsible attitude towards technology and internet use.

Unit 4.6 – We are careful when talking to virtual friends

Virtual friendship vs real friendship; who we can trust

Children learn what is meant by virtual friendship and how this differs from real-life friendship. They discuss the places people might meet virtual friends and then test a virtual friendship with a real friendship.

Online safety focus:

• Understand that virtual friends are still strangers that they do not know.

• Apply their knowledge of online safety to decide what information they, as virtual friends, can safely share online.

• Recap rules for reporting suspicious or uncomfortable online situations.

Year Five E-Safety Overview

Unit 5.1 – We are Year 5 rule writers

Reviewing and editing our online safety rules

Children recall their learning from the previous year's online safety lessons and then review different online safety scenarios to decide on the best response to these.

They then review, discuss and edit the online safety rules they created in Year 4.

Online safety focus:

· Consider online safety scenarios encountered in Year 4 (both at school and at home) and appreciate how these new experiences can be used to update their online safety rules.

· Consider what new strategies they can apply to online safety scenarios, such as clicking the CEOP 'Report abuse' button.

· Review and edit their online safety guidelines.

· Develop their online safety rules so they are easily understood and appropriate for Year 5 pupils.

Unit 5.2 – We are responsible for our online actions

Understanding the impact of online behaviour

Children learn that we must take responsibility for our own actions regardless of what others are doing.

They take on the role of one of six characters in an online safety scenario and decide how each character should respond to the situation.

Online safety focus:

• Recognise that online behaviour can have real life negative effects on other people.

• Understand that we must take responsibility for our own actions online, regardless of what other people are doing.

• Critically assess all information surrounding an online safety scenario to decide whether it constitutes online bullying.

• Use their knowledge of online safety to reach a consensus on the appropriate response to an online incident.

Unit 5.3 – We are content evaluators

Understanding advertising and endorsements online

Children discover that some online content creators are paid by companies to support their products. They learn to ask probing questions about online content and go on to create a simple rap or rhyming saying to remind them of ways of being discerning when viewing content online.

Online safety focus:

• Understand that some people get paid to endorse products online.

• Develop a discerning attitude to online content so that they can confidently reach their own conclusions.

Appreciate the value of trusted adults in helping them reach an informed conclusion.

Unit 5.4 – We are protecting our online reputation

Developing strategies to protect our future selves

Children learn that posting inappropriate, rude or offensive content online can affect our online reputation.

Through role-play, they discover the consequences of posting inappropriate content online.

Online safety focus:

• Understand that posting inappropriate information online can cause regret later.

• Understand how to manage their online reputation.

• Understand that, although information posted on the internet might not always be true or accurate, it can last forever.

• Understand that it is possible to search the internet for information about particular individuals.

Unit 5.5 – We are respectful of copyright

Understanding and applying copyright laws

Children learn that copyright rules exist to protect original content creators. They review a scenario to work out if copyright rules apply and what the rights and responsibilities are of the parties involved.

They then review how copyrighted content could be used in school, and provide alternatives for this.

Online safety focus:

• Understand that copyright laws exist to protect original content creators.

• Understand that content they choose to use or upload on the internet may be subject to copyright laws.

• Further develop their understanding of rights and responsibilities as digital citizens.

Unit 5.6 – We are game changers

Understanding how games developers make money

Children discover the different ways that game developers ensure their games are successful and make money. They learn strategies to help guide them when selecting and playing online games and apply their knowledge to create a safe online gaming guide for families.

Online safety focus:

• Understand different business models for online games.

• Understand that accounts for devices are linked to real-life bank accounts.

• Understand that some features in online games and apps cost real money.

• Understand that research, parental controls and device settings are tools we can use to help us game confidently.

Year Six E-Safety Overview

Unit 6.1 – We are online safety ambassadors

Reviewing and editing our online safety rules

Children look at the use of 'Report this' functionality within websites and apps before considering appropriate responses to online safety scenarios specific to them. They will then consider how online safety rules for their class could be made more relevant for their age groups, in response to these new scenarios.

Online safety focus:

· Consider online safety scenarios encountered in Year 5 (both at school and at home) and appreciate how these new experiences can be used to update their online safety rules.

· Consider what new strategies they can apply to online safety scenarios, such as using reporting buttons within websites and apps.

· Review and edit their online safety guidelines.

· Develop their online safety rules so they are easily understood and appropriate for Year 6 pupils.

Unit 6.2 – We will not share inappropriate images

Inappropriate use of technology and the internet – nude selfies

Children learn about the risks, responsibilities and consequences of sharing inappropriate images including nude selfies. They discuss the reasons why people might post such selfies and offer advice to two children who are considering sharing nude selfies.

Online safety focus:

• Understand the negative consequences of sharing nude selfies.

• Develop confidence in saying no when they are posed with a request for inappropriate and/or indecent images of themselves.

• Understand that once an image is online, it stays online forever.

Unit 6.3 – We are safe social networkers

Understanding that internet safety skills must always be switched on

Children learn that most popular networking sites have age restrictions which should be adhered to. They discuss the ways of reducing the risks of using social networking sites and go on to develop a personal memo to remind them how to minimise these risks.

Online safety focus:

• Understand that most online sites and apps require an account holder to be a minimum of 13 years old.

• Understand that they should check and adhere to the age restrictions of a site or app.

• Understand why age restrictions apply to online communication tools.

• Develop resilience to online behaviour and influences in an unfamiliar setting.

Learn how to use appropriate social networking sites safely.

Unit 6.4 – We are respectful of others

Respecting the personal information and privacy of others

Children learn that everyone has a right to privacy and that they need to be mindful of protecting other people's personal information online. They consider situations where we must be mindful of the privacy preferences of others and then create a permission pledge for their family.

Online safety focus:

• Consider online safety scenarios encountered in Year 5 (both at school and at home) and appreciate how these new experiences can be used to update their online safety rules.

• Consider what new strategies they can apply to online safety scenarios, such as using reporting buttons within websites and apps.

• Review and edit their online safety guidelines.

• Develop their online safety rules so they are easily understood and appropriate for Year 6 pupils.

Unit 6.5 – We are online safety problem solvers

Using our skills to resolve unfamiliar situations

In this unit, children will develop confidence in responding to unfamiliar online safety scenarios, in preparation for moving on to secondary education. Children will be presented with three unfamiliar online safety scenarios and have to develop an appropriate response to each.

Online safety focus:

• Develop confidence in their ability to act appropriately when confronted with unfamiliar situations involving technology and the internet.

• Revisit the key concepts of digital citizenship.

Unit 6.6 – We are safe gaming experts

Creating and delivering advice on safe online gaming

In this unit, children will learn about the possible online safety risks of online gaming, including exposure to inappropriate content, bullying and trolling, and bribery. Children will then use what they have learnt to plan an assembly or presentation around safe gaming advice for parents, children or teachers.

Online safety focus:

• Understand the risks involved with online gaming, including exposure to inappropriate content, grooming, bullying, trolling and the use of bribery tactics.

• Understand that research and parental controls and device settings are tools we can use to help us game safely and confidently.

• Apply their knowledge of safe gaming practices to plan and deliver an assembly to other children and/or parents.

• Consolidate everything they have learnt about age- appropriate online gaming in preparation for their transition to KS3.