Queen Eleanor's Church of England Junior School
An Academy in the Good Shepherd Trust
Queen Eleanor's Road, Onslow Village,
Guildford, GU2 7SD

Internet Safety Policy

Date	Review Date	Coordinator
September 2023	September 2024	Computing Coordinator

Outline

Internet Safety Policy

Internet Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Internet safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools' and other statutory documents.

Aims of the Internet Safety Policy

This policy aims to do the following:

- Set out expectations for all Queen Eleanor's C of E Junior School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).

- Help all participants to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.

- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.

- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  -for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  -for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Main Risks

What are the main Internet Safety risks today?

- Internet Safety risks are traditionally categorised as one of the 4 Cs:

Content – being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism' (KCSIE 2023).
Contact – being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes' (KCSIE 2023).
Conduct –personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying' (KCSIE 2023).
Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams' (KCSIE 2023).

- These 4 areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

What does electronic communication include?

- **Internet collaboration tools** (e.g. social networking sites, blogs)
- **Internet Research** (e.g. web sites, search engines and Web browsers)
- **Mobile Phones and personal digital assistants**
- **Internet communications** (e.g. E-mail and Instant Messaging)
- **Webcams and videoconferencing**

Reducing Online Risks

- The school recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

- We will do the following:

-Regularly review the methods used to identify, assess and minimise online risks.
-Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
-Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
-Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

-All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.

Teaching and Learning

End-to-End Internet Safety

Internet Safety depends on effective practice at a number of levels:

- Responsible computing use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of Internet Safety policy in both administration and curriculum, including secure school network design and use.

The following subjects have the clearest online safety links:

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- Computing
- Citizenship

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place). Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents. At Queen Eleanor's C of E Junior School, we recognise that Internet safety and broader digital resilience must be thread throughout the curriculum.

Why internet and digital communications are important…

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet use can enhance learning in a number of different ways.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content…

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant internet content e.g. they should tell a member of staff. For pupils whose parents lack economic or cultural educational resources, the school should build digital skills and resilience acknowledging the lack of experience and internet at home.
- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.
- Using the Kapow scheme of work, the online safety curriculum is provided as part of the Computing curriculum and will be regularly revisited throughout the academic year. As part of the scheme children will have a specific online safety lesson once every half term.
- Key online safety messages should be reinforced as part of a planned programme of collective worship (at least twice a year by a member of staff and the school will participate in Safer Internet Day every year).
- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Internet Safety rules will be displayed in school.

Vulnerable Pupils

- The school is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to, children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.

- The school will seek input from specialist staff as appropriate, including the SENCO/HSLW or PSHE Leader.

Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Pupils will be advised to do the following:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.

- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within school and externally.

Internet use - Possible teaching and learning activities

Activities	Key Internet Safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Webquest UK SE grid for Learning
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	• Ask Jeeves for kids • Yahooligans • CBBC Search • Kidsclick • swiggle.org.uk • Q-files.com • dkfindout.com/uk/
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils will only email other pupils. Pupils should never give out personal information. Class Teachers will manage emails sent directly to experts.	RM Unify email accounts to be used Purple Mash email activities used with pupils
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News Headline History SE Grid for Learning Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News Learning grids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	Skype Flash Meeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype Flash Meeting National Archives "On-Line" Natural History Museum Imperial War Museum

Managing Internet Access

Information system security

- School Computing systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed

E-mail

- Staff may only use approved e-mail accounts on the school system.
- Online staff to pupil communication must only take place within the learning platform being used and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- E-mail sent to an external organisation should be written carefully and authorised before sending, if appropriate, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- The official *school* e-mail service must be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about internet safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Managing filtering

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place, and regularly review their effectiveness." Ensuring they are "doing all that they reasonably can to limit children's exposure to the above risks from the school's IT system" but at the same time "block harmful and inappropriate content without unreasonably impacting teaching and learning."

- The school will work with Surrey County Council and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Internet Safety Coordinator/School technician.

- Senior staff will ensure that termly checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A log of any incidents will be kept on the school Internet Safety Incident form (see appendix 5) in order to identify patterns and behaviours of the pupils.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will be issued with a school phone where contact with parents or pupils is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.
- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child protection, Data security and Acceptable use.
- Staff will be advised to:
  -Keep mobile phones and personal devices in a safe and secure place during lesson time.
  -Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  -Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  -Not use personal devices during teaching periods, unless permission has been given by the head teacher, such as in emergency circumstances.
  -Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
  -Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead or head teacher.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
  -To take photos or videos of pupils and will only use work-provided equipment for this purpose.
  -Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy

-If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Management of Applications (apps) used to Record Children's Progress

- The school uses Arbor to track pupil's progress and share appropriate information with parents and carers.
- The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation.
- In order to safeguard pupils data:
  -Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
  -Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
  -School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
  -All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

Publishing

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Senior Leadership Team will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Publishing pupil's images and work

- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained in the global permission form at the start of the school year.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- Pupils' work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Internet Safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. These skills will be revisited and developed for example in Year 4 pupils will look at appropriate online behaviours expected of themselves and others, whilst in year 6 pupils will look at how to capture and collect evidence of online bullying. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to introduce the Children's Commission Digital 5 A Day.

The school has an official Twitter account (managed by the Phase Leaders/SLT) and is updated regularly. Email is the official electronic communication channel between parents and the school, and between staff and pupils.

Staff Publishing

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

-Setting the privacy levels of their personal sites as strictly as they can.
-Being aware of location sharing services.
-Opting out of public listings on social networking sites.
-Logging out of accounts after use.
-Keeping passwords safe and confidential.
-Ensuring staff do not represent their personal views as that of the school.

- Members of staff are encouraged not to identify themselves as employees of the school on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communication

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the head teacher.
- If on-going contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the head of school.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

Personal Devices and Emails

Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the schools code of conduct.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

Staff

- The use of personal email addresses by staff for any official school business is not permitted.
- All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

CCTV

- The school may use CCTV in some areas of school property as a security measure.
- Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation

Policy Decisions

Protecting personal data

- The School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct and Acceptable Use' before using any school computing resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents and children will be asked to sign and return a consent form.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor GST can accept liability for the material accessed, or any consequences of Internet access.
- The school will monitor Computing use to establish if the Internet Safety policy is adequate and that the implementation of the Internet Safety policy is appropriate and effective.

Handling Internet Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.

- Complaints of a child protection nature must be dealt with in accordance with school's child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  -Internal response or discipline procedures
  -Involvement by Local Authority / Academy Group or national / local organisation (as relevant). -Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include: -incidents of 'grooming' behaviour
  -the sending of obscene materials to a child
  -adult material which potentially breaches the Obscene Publications Act
  -criminally racist material
  -promotion of terrorism or extremism
  -other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is vital that all staff recognise that Internet Safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem. Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with Internet Safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Sexual Harassment / Peer on Peer Abuse Policy (if separate)
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc.)

This school commits to take all reasonable precautions to ensure Internet Safety, but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes. Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Head teacher, unless the concern is about the Head teacher in which case the compliant is referred to the GST Chair of trustee Directors. If unavailable, then the LADO (Local Authority's Designated Officer) will be contacted directly. Staff may also use the NSPCC Whistleblowing Helpline (displayed in school). The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Community use of the Internet

- All use of the school internet connection by community and other organisations shall be in accordance with the school Internet Safety policy.

Communications Policy

Introducing the Internet Safety policy to pupils

- Appropriate elements of the Internet Safety policy will be shared with pupils.
- Internet Safety rules will be posted in school and discussed with the pupils throughout the year.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of Internet Safety issues and how best to deal with them will be provided for pupils. This will be addressed each year as pupils become more mature and the nature of newer risks can be identified.
- Pupils will be taught about Internet Safety every half term during the Computing curriculum as well as being referenced during wider curriculum activities.
- The whole school will participate in Internet Safety Day each year.

Staff and the Internet Safety policy

- All staff will be given the school Internet Safety policy and its importance explained.
- All staff will sign to acknowledge that they have read and understood the Internet Safety policy and agree to work within the agreed guidelines.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor Computing use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' attention will be drawn to the School Internet Safety Policy in newsletters, the Parent Handbook and on the school website.
- The school will ask all new parents to sign the parent/pupils agreement when they register the child with the school.

Risk Behaviours

Online grooming and child abuse

- The school will ensure that all members of the community are aware of online child sexual abuse, including: youth-protected sexual imagery, exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is available to pupils and other members of the school community.

There are a number of illegal actions that adults can engage in online that put children at risk:

- Swapping child abuse images in chat areas or through instant messenger with other adults or young people and forming networks with other child abusers to share tips on how to groom more effectively and how to avoid being caught
- Swapping personal information of children that they have collected with other abusers
- Participating in online communities such as blogs, forums and chat rooms with the intention to groom children, collect sexually explicit images and meet them to have sex.

Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
  -Act in accordance with the school's Child protection and Safeguarding policies.
  -Immediately notify the Designated Safeguarding Lead.
  -Store any devices involved securely.
  -Immediately inform the police via 101 (or 999 if a child is at immediate risk)
  -Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  -Inform parents/carers about the incident and how it is being managed.
  -Make a referral to Specialist Children's Services (if required/ appropriate).
  -Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
  -Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.

- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
  -Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or the Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from the Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- The school will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Police and/or the Education Safeguarding Team.

- If made aware of IIOC, the school will:
  -Act in accordance with the schools child protection and safeguarding policy and procedures.

-Immediately notify the school Designated Safeguard Lead.
-Store any devices involved securely.
-Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), the police or the LADO.

- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
  -Ensure that the Designated Safeguard Lead is informed.
  -Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  -Ensure that any copies that exist of the image, for example in emails, are deleted.
  -Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the school devices, the school will:

-Ensure that the Designated Safeguard Lead is informed.

-Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

-Ensure that any copies that exist of the image, for example in emails, are deleted.

-Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).

-Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

-Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:

-Ensure that the head of school is informed.

-Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.

-Quarantine any devices until police advice has been sought.

Youth-Protected Sexual Imagery

- This refers to images and video footage that is either owned, shared or created by young people under the age of 18.
- The school will take all reasonable precautions to ensure that children are safe from youth-protected sexual imagery while accessing the internet.
- 'Sexting' is illegal – but that doesn't mean a criminal conviction. Even though it's legal to have sex at 16, it is illegal to create or share sexually explicit images of people under the age of 18, even if the person in the picture is you. The law was designed to protect children – in the UK, this is anyone under the age of 18 – from adult sexual predators, not to criminalise teenagers for exploring their sexual feelings. Previously, if a school found out pupils under 18 had been sharing such images, even consensually between partners, they had to inform the police.

- The guidance now advises that if the school believes that coercion or abuse has not occurred, they can handle the incident internally. If the school does refer the incident to the police, they will investigate and it may result in a criminal conviction or, more likely, become what is known as an outcome 21**.**

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at this school.

Cyberbullying is when someone bullies others using electronic means, this might involve social media and messaging services on the internet, accessed on a mobile phone, tablet or gaming platform. The behaviour is usually repeated. Like any form of bullying, cyberbullying can be horrible for the children involved and hard for them to talk about.

Cyberbullying can happen via text, email and on social networks and gaming platforms. It can consist of:

- Threats and intimidation
- Harassment and stalking
- Defamation
- Rejection and exclusion
- Identify theft, hacking into social media accounts and impersonation
- Publically posting

Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at this school and will be responded to in line with existing school policies, including Antibullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through C-SPA and/or the Police.

Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Head of school will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

Sexting

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called 'Sharing nudes and semi-nudes; how to respond to an incident' for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area. The documents referenced

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying.
Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Responding to an Internet Safety Incident

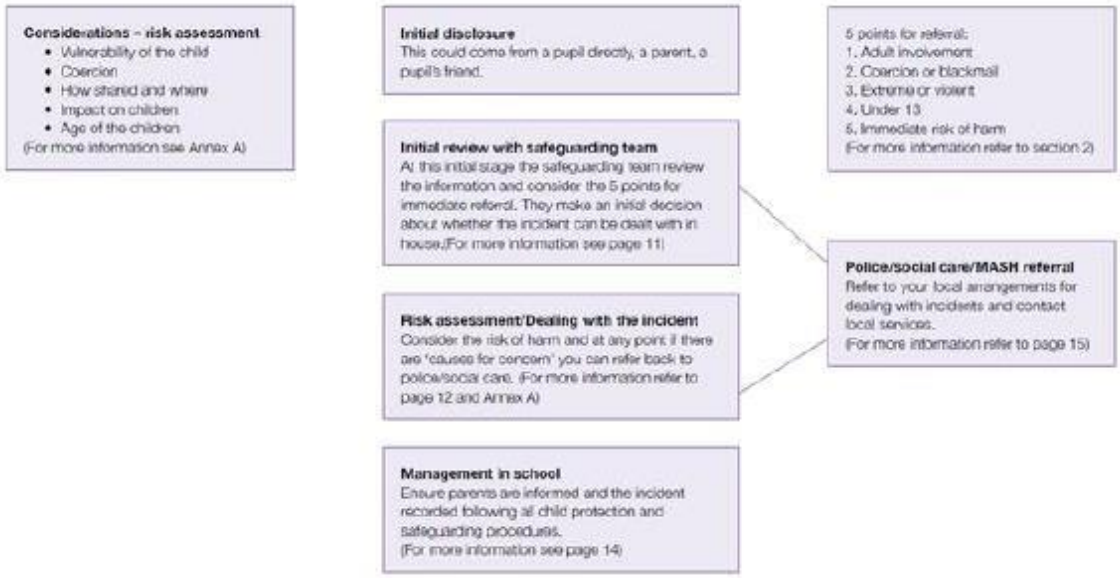
- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyber bullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
- Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the C-SPA.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or the Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

This guidance is for senior management within schools on how to respond to an Internet Safety incident of concern. It is important to note that incidents may involve an adult or child as the victim or the instigator. Adults are also subject to cyber bullying by pupils.

The first section outlines key Internet Safety risk behaviours. The flowchart illustrates the approach to investigating an incident of concern. This diagram should be used with the screening tool and the Surrey Child Protection Procedures, which include what to do if you are concerned about a child, or about an adult working with children. Schools' DSLs will be conversant with these and the processes for referral.

Annex G

Flowchart for responding to incidents



INTERNET SAFETY INCIDENT REPORT

This form is for reporting any Internet Safety incident that occurs at school or outside of school but could have implications for the school. It is linked to the Internet Safety Policy.

Adult making report: _____ Date: _____

Children involved: _____ Class: _____

Time: _____

Nature of incident?	
Description of the incident that caused the concern.	
What happened as a result of the incident?	
Consequences and actions that were taken following the incident.	
Monitoring that is required and by whom?	
Discussed with / Circulated to:	Class Teachers, SLT, MLT, Teaching Assistants, Office Staff, Parents, Pupils, Computing Technician, Area Schools Support Team, Police, Other (please specify)

Circulated By: _____ Date: _____

Appendix 4: Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Internet Policy and Internet Code of Conduct for further information and clarification.

1. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead.
2. I understand the responsibilities listed for my role in the school's Online Safety policy and agree to abide by these.
3. The information systems are school property and I understand that they must be used appropriately in school. I agree to follow school guidelines as detailed in the Internet Policy and E-Learning Code of Conduct with regard to use of school information systems.
4. I will ensure that my information systems use will always be compatible with my professional role.
5. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, is monitored/captured/viewed by these systems and/or relevant/authorised staff members.
6. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:

-not sharing other's images or details without permission

-refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

7. I understand that school information systems may not be used extensively for private purposes, without specific permission from the head teacher.
8. I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
9. I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager and I will follow the data protection regulations for staff.
10. I will only install new software or hardware with permission from the IT technician or IT leader.
11. I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the data protection regulation.
12. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
13. I will respect copyright and intellectual property rights.
14. I will report any incidents of concern regarding children's safety to the school IT leader or the head teacher as appropriate.
15. I will ensure that any electronic communications with pupils are compatible with my professional role.
16. I will promote Internet Safety with pupils in my care and will help them to develop a responsible attitude to system use regarding the content they access or create and to help them to stay safe in this environment.
17. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school -approved and school-monitored

ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the head teacher.

18. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
19. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either.
20. I will not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with my professional role.
21. I will not accept current school pupils as friends on social networking spaces such as Facebook and I will not accept past pupils under 18 without the express permission of their parents.
22. Regarding social media, I will ensure that my privacy settings on all social networking sites are at an appropriate level and I understand that I must remain professional when accessing or interacting with social networking sites out of school hours. The use of social media will remain as part of my social life and I will not make any references to my place of work, any activities within the school or any work concerns that I may have.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Any reports of the inappropriate use of social media that are brought to the attention of school leaders will be investigated and may result in disciplinary action being taken.

Appendix 5: Data Protections Regulations for Staff

The General Data Protection Regulations (GDPR) forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018) which came in effect from 25 May 2018.

The following data protections arrangements must be read in conjunction with the GDPR presentation and must be followed at all times.

1. Password security

1.1 Passwords must contain a minimum of 8 characters; one of which must be a number, one must be a capital letter and one must be a lower case letter.
1.2 Do not use obvious passwords e.g Password1 – Arbors will reject obvious passwords automatically. Consider using a password with three random words combined e.g. Horsemanflower1
1.2 You will be forced to change your server password regularly. When the server password is changed you must change Arbor password at the same time. To change the Arbor password click the options (small cog icon at the top right) and click reset password.
1.4 Do not allow your computer / electronic devices (either at home or in school) to save passwords – if this happens automatically this must be reported to the IT technician and rectified.
1.5 Passwords must not be shared, given to anyone other than the IT technician or given over the phone; Arbor's support team will never ask for a password. In exceptional circumstances a password may be shared by more

than one member of staff but this must be approved by the IT technician and the password must remain only with those staff members authorised to have it. The only circumstances in which this will apply are sharing of a generic email address e.g. After school club@, parents@ etc. Arbor passwords must never be shared.
1.6 Passwords must not be written down, for example in your diary. Any document with a list of passwords must be stored safely e.g. in a locked filing cabinet or password protected if stored on the computer.

2. Data Security

2.1 When using any electronic device (either at home or at school), you must log off or Ctl Alt Del and lock the device when you leave it.
2.2 If you allow any other member of staff to use a PC logged on in your name, be aware that any confidential documents within your personal H drive will be available for them to open. Also be aware that if you allow a member of staff to use your Arbor account which you have logged on for them, you are ultimately responsible for any work carried out in your name.
2.3 The Arbor system contains all personal and sensitive data for all pupils in the school. You must therefore use it with the utmost care by ensuring that only authorised individuals are able to log on and view data.

3. Remote access

Teachers have access to log onto the server from any device remotely. The following protocols to ensure that data is not compromised, must be followed at all times:
3.1 Instructions regarding the use of passwords must be followed at all times.
3.2 When using the link to access the server remotely, **never** tick the "Remember by credentials" box.
3.3 When logged on remotely, you should only be connected whilst actually working at the computer. If you walk away from your computer for any reason whilst you are logged on remotely, you must log off.
3.4 Ensure that all instructions are followed, in particular ensuring that you log off correctly at the end of your session or your data will not be saved.
3.5 Your home PC must have up to date anti-virus protection installed
3.6 You must not use memory sticks or any external hard drives for transferring data.
3.7 In exceptional circumstances, an encrypted memory stick may be used with the permission of the school business manager. If such a device is used, a list of all documents that contain personal data (and the nature of the personal data) of pupils or staff must be kept and maintained so that it is always up to date.
3.8 Any hard files or electronic devices being taken home must not be left in a car.

4. Breaches of security

4.1 Any concerns regarding breaches of data security must be reported immediately to the IT technician and a member of SLT. If unsure, please report concerns. These may include: misuse of passwords, loss of data, loss or damage of any electronic device on which data is stored, loss of any hard files containing personal data etc.