Online Safety Policy

September 2024

ST CHRISTOPHER'S
HAMPSTEAD

ONLINE SAFETY POLICY

Policy to be reviewed annually			
Action	**Owner**	**Date**	**Completed**
Reviewed	Online Safety Coordinator	September 2024	✓
Reported	Risk & Compliance Committee		
Approved	Board of Governors		

To be published on	
School network	✓
School website	✓
ISI Portal	✓

Accessibility notice

To enable easier reading, this Policy is available in a larger font upon request.

1. Key Contacts

Head	**Mark Maddocks** **Ext 215** **mark.maddocks@stchristophers.london**
Online Safety Coordinator	**Holly Thomas** **Ext 207** **Holly.thomas@stchristophers.london**
IT systems	**EAC** **Ext 236 (Tuesdays/Thursdays)** **tech.support@eac-ns.co.uk**
Designated Safeguarding Lead	**E**lizabeth Courtney-Magee **Ext 241** **elizabeth.courtney-magee@stchristophers.london** **dsl@stchristophers.london**
Nominated Governor	**Sarah Kavanaugh** **Sarah.kavanaugh@stchristophers.london**

London Borough of Camden

Child protection service manager:

Name: Kurt Ferdinand

Contact details: 020 7974 6481

Local Authority Designated Officer (LADO):

Name: Jacqueline Fearon

Contact: 0202 7974 4556

Email: LADO@camden.gov.uk

Child and Family Contact/MASH team:

Service Manager: Tracey Murphy

Tel: 020 7974 1553/3317

Camden online safety officer:

Name: Jenni Spencer

Tel: 020 7974 2866

Prevent Co-ordinator/ Education Manager

Name: Jane Murphy

Tel: 020 7974 1008

2. Aims and Objectives

St Christopher's School is committed to safeguarding and promoting the welfare of children and young people and this extends to pupils' use of technology and their online interactions.

We recognise that in an ever-evolving world that technology is becoming increasingly more accessible as a learning tool in all primary year levels. We identify the benefits of providing learners with the opportunity to use and access these technologies to enhance their learning experiences. We do also understand that with greater access to technology comes risk and danger to young people and concerns can occur both online and offline simultaneously or separately.

We therefore aim to:

- Ensure that online safeguarding forms an integral part of planning and teaching
- Promote a culture of safe practice and awareness of the standards of online behaviours that is embedded across the curriculum
- Teach our pupils how to stay safe online and how to avoid making themselves vulnerable to a range of risks linked to 'Content, Contact, Conduct, and Commerce'
- Enable pupils to talk and express their feelings about online safety within a safe environment
- Encourage partnerships with parents, staff and pupils in our coverage of online safety
- Promote responsible and effective use of digital and online communication (including the use of the internet, social media, mobile phones and digital technology).
- Establish clear procedures to allow teachers to identify, intervene and escalate an incident, where appropriate
- Ensure that consistent messages are given to staff and pupils and that adequate training takes place on a regular basis
- Ensure staff are aware of school policies pertaining to use of technology and that their own practices align

We recognise that digital and online safety is an extension of our wider commitment to safeguarding, therefore this policy draws together the principles and practices set out in a number of other policies and should be read in conjunction with the documents below:

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Artificial Intelligence Policy
- Behaviour Policy
- PSHCE Policy

- Digital Technology Policy
- Staff Acceptable Use Policy
- Pupil Acceptable Use Agreement (See appendix 1)
- Data Protection and Privacy Policy
- Pupil Searches and Confiscation Policy
- IT Policy

3. Risks online

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

- Content: being exposed to illegal, inappropriate or harmful content, such as pornography, fake news or information advocating violence, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, illegal and anti-social behaviour which the pupils are not able to evaluate in a critical manner
- Contact: being subjected to harmful online interaction (e.g., in chat rooms, gaming site and other social networking sites) with other users, such as 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
- Conduct (or culture): personal online behaviour and use of mobile devices for the purposes of sexual harassment such as 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 and child-on-child abuse; using information from the internet in a way that breaches copyright laws; and
- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams, fraud or identity theft

In practical terms, the main online risks have been identified as:

- Breach of privacy (data misuse; identify theft; oversharing)
- Grooming and inappropriate contact with strangers
- Cyberbullying
- Access to sexual images
- Fraud and allowing or seeking unauthorised access to personal information or private data
- Infringement of copyright, plagiarism and unlawful downloading of content
- An inability to evaluate the quality, accuracy, and relevance of information, particularly with regarding concerns around AI generated content, , and the ability to be drawn into echo chambers
- The potential for excessive or addictive use which may impact on social and emotional development and/or learning

4. Procedures

School procedures

We ensure that there are clear procedures for the restriction of unwanted online activity, and actions to follow in the event of an online safety related issues arising:

- Limit pupils' exposure to the above risks within the school's IT system by using robust filtering and monitoring systems on school devices and networks (SENSO/Sophos). These safeguards will be regularly checked by our IT staff and with the DSL responsible for monitoring notifications.
- Ensure appropriate mechanisms for staff, pupils, and parents to report issues or concerns and that any concern is dealt with appropriately in accordance with the Child Protection and Safeguarding policy.
- Investigate any potential incidence of child-on-child abuse, including bullying, harassment or threatening behaviour in accordance with the Behaviour policy and Anti-Bullying policy.
- Investigate any incident that may breach the Pupil Acceptable Use policy or the Staff Acceptable Use Policy, the Behaviour Policy and the Child Protection and Safeguarding Policy.

Reporting and Monitoring Concerns:

Pupils are to report online safety concerns to a trusted adult and staff are to report online safety concerns to the online safety coordinator and designated safeguarding lead as well as logging them on CPOMS. Any concerns raised by parents are to be logged directly on CPOMS, with any accompanying email correspondence and followed up by the staff member involved as well as the online safety coordinator and designated safeguarding lead. It is the Head and DSL's responsibility to monitor staff devices through SENSO. If they have any concerns about a staff member, they will report them to the governors.

Access to third party online resources

Third party online resources include, for example: websites, apps, channels, and internet connectivity solutions.

While we are able to manage the settings and configuration of our own network, equipment and systems, the internet provides its own opportunities and challenges in terms of privacy, online safety, security and protection. When engaging with third party online resources that are not within the school's control, the following must be taken into account:

- These must not be used by the students unless they are approved by the school.
- Particular attention should be paid to the following:
    - Age restrictions relating to the resource
    - Staff should never endorse or recommend resources that they have not fully checked, nor submitted to the IT Team for approval

Mobile phones and portable electronic devices

Pupils may not use mobile phones and portable electronic devices as outlined in the school Pupil Acceptable Use policy. Pupils have access to online resources using school devices, exclusively using

the school's Wi-Fi network. School devices do not connect to 3G, 4G, or 5G. The only occasion where a pupil can have a mobile phone is in Year 6 for the purpose of walking to and/or from school. The procedure for the management of these devices can be found in the Pupil Acceptable Use Policy. If the pupil does not follow procedure, the school cannot be held responsible if the device goes missing.

Examining Electronic Devices

The Head/DSL can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the head and head of upper school or lower school to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance

on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy in conjunction with our pupil searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 12 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time (this policy has been applied by our IT Team)
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates when prompted

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice the IT Team (EAC)

Cyberbullying

The internet and social networking sites must not be used to hurt, humiliate, slander or defame another person. Pupils are made aware that actions in this regard undertaken outside of school may also contravene school policies and so may be subject to school sanctions (in the first instance). The same sanctions will apply to incidents of cyberbullying as would apply to any other form of bullying.

We recognise that many pupils have mobile phones and access to the internet outside school and to that end:

- The school holds an Internet Safety week each year, in which the risks of technology and cyber bullying are discussed in depth. The school arranges internet safety workshops, addressing the safe use of the internet and mobile phones

- Acceptable Use Policies are reviewed annually with all pupils in school and at home, so that they have a good understanding of how they must behave online
- The Head and safeguarding team update policies and provide parents with advice, helping them to understand how children can use technology safely, as well as the risks and consequences of online platform usage
- Staff have a duty to make sure that they are familiar with their role in dealing with cyber bullying
- Victims should keep emails and text as evidence for tracing and possible police action. Such evidence is to not be forwarded or used until a discussion has taken place between relevant parties.

Acceptable Use Agreements

All pupils, parents, staff, volunteers and governors are expected to read and abide by an agreement regarding the acceptable use of the school's online systems. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We monitor all school owned devices as well as the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

How the School will respond to misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in this policy as well as (where applicable) our Anti-bullying Policy, Behaviour policy and Acceptable Use policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct and staff Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Artificial Intelligence:

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Microsoft CoPilot. We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils in line with our anti-bullying policy and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment and seek permission from our Head of IT and IT Team (EAC) where new AI tools are being used by the school.

5. Roles and Responsibilities

All staff, governors and volunteers have a duty to protect children from abuse and to report matters of concern to the Designated Safeguarding Lead (see the Child Protection and Safeguarding Policy). In addition, the following roles have specific areas of responsibility relating to online safety:

Online Safety Coordinator: Holly Thomas

- The Online Safety Coordinator takes lead responsibility for online safety in school, in particular:
    - Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
    - Working with the Head, Designated Safeguarding Lead, IT staff the nominated governor and other staff, as necessary, to address any online safety issues or incidents and to ensure that the school has appropriate filtering and monitoring systems
    - Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
    - Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's Behaviour Policy
    - Updating and delivering staff training on online safety
    - Organising parents' discussion evenings on the topic of digital and online safety
    - Supporting form and digital technology teachers to deliver the online safety component of the digital technology curriculum
    - Support the Heads of Lower School and Upper School in any pastoral and disciplinary response as and when needed in the case of an online safety concern
    - Liaising with the Head of Digital Technology and PSHCE Coordinator to write the online safety curriculum

Designated Safeguarding Lead: Elizabeth Courtney-Magee

- The DSL works closely in conjunction with the Online Safety Coordinator and oversees all safeguarding matters concerning online safety
- In collaboration with the Online Safety Coordinator, the DSL ensures any online safety incidents, including monitoring alerts, are reported and dealt with appropriately informing appropriate parties where necessary
- In collaboration with the Online Safety Coordinator, the DSL organises appropriate training and education for staff, students and the parent body
- Reviews and updates policies, procedures and documentation relating to safeguarding and child protection
- Coordinates pastoral and disciplinary response as and when needed in the case of an online safety concern

IT Manager (third party contractor EAC)

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while 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
- Conducting a full security check and monitoring the school's ICT systems on a termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensure staff and pupil devices have anti-virus and anti-spyware software installed on them
- Ensure staff and pupil's hard drives are encrypted

Other Members of the Safeguarding team: Amy Ullman, Stephanie Martineau and Jennie McGovern, James Greene

- Supports the DSL and Online Safety Coordinator in any matters arising

Head of IT and Digital Innovation: Holly Thomas

- Oversees the digital technology curriculum and a programme for development of digital skills
- Develops and delivers the digital technology curriculum
- Delivers information on digital learning and technology use to staff, governors, and parentsManages the safety and security of the school's technical infrastructure in conjunction with EAC
- Manages the school's network filtering and monitoring systems
-

Head of PSHCE: Stephanie Coyle

- Develops and oversees the delivery of the PSHCE curriculum

Form teachers

- Deliver PSHCE curriculum
- Monitor and report any pastoral concerns using CPOMs arising out of their conversations with pupils, staff or parents
- Communicate the school's Online Safety and Acceptable Use policy to pupils

Role of all Staff

- Adhere to our Online Safety and Acceptable Use Policy and procedures
- Familiarise and understand the role and responsibilities of their own technology use as outlined in the staff Acceptable Use Policy
- Report any breaches of online technology use to the Online Safety Coordinator and Designated Safeguarding Lead
- Be vigilant in supervision of pupils' internet use through the use of SENSO's screen monitoring tool

- Be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications

Role of Governors

- Governors have a statutory responsibility for pupil safety and should therefore be aware of online safety issues, providing support to the Head in the development of the school's online safety strategy.
- Governors should ensure that there are policies and procedures in place to keep pupils safe online and that these are reviewed regularly.
- Governors should liaise with IT staff and service providers to annually review school IT filtering and monitoring systems to check their effectiveness and ensure that the school leadership team are aware of what provision is in place and how to escalate any concerns.
- Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use business email addresses when conducting school business.

- **Pupils with Special Educational Needs**

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. The School should have a flexible and personalised approach to online safeguarding for these pupils in order to meet their needs.

The **Learning Enrichment Coordinator** is responsible for providing extra support for these pupils and should:

- Link with the online safety co-ordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with SEND
- Where necessary, liaise with the online safety co-ordinator and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with SEND
- Ensure that the school's online safety policy is adapted to suit the needs of pupils with SEND
- Be aware that some pupils with SEND may not have the cognitive understanding to differentiate between fact and fiction online and may repeat content and behaviours in the real world without understanding the consequences
- Liaise with parents, carers and other relevant agencies in developing online safety practices for pupils with SEND
- Keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with SEND.

Online Safety Education and Training

Teaching and Learning

At St Christopher's School, online safety is embedded in our teaching across the curriculum. It is taught in an atmosphere of trust and is intrinsically linked to our safeguarding agenda and connected to our Pupils' Acceptable Use Policy, to ensure that we are promoting the welfare of our pupils online.

The safe use of technology is taught to pupils of all ages through digital technology and PSHCE lessons, presentations, assemblies and form time discussions. Teachers employ a wide range of strategies when teaching online safety, with interactive talking activities encouraged in PSHCE and online safety resources used as the focus for learning in digital technology. Our aim is that online safety skills are not just developed during specific lessons but are also reviewed as and when issues arise.

SMSC – Spiritual, Moral, Social and Cultural development

SMSC education is important within the online safety curriculum as pupils are encouraged to share their experiences and question the technology that they are using. News stories and current events are a valuable tool when discussing and promoting safety online.

Child-initiated Learning

The online safety curriculum is child-centred and flexible, allowing the ideas and needs of the pupils to be effectively facilitated. Pupil input is paramount when planning effective safety lessons and open discussions are encouraged.

In Reception and Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of their time at St Christopher's, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Staff

The Staff Code of Conduct and staff Acceptable Use Policy, provide guidelines on how staff should behave and interact with students. All new staff receive a safeguarding induction as well as an online safety induction which includes guidelines on how staff should behave when online. Staff acknowledge that they have read and understood both documents referred to above and they are reviewed annually. This procedure is also in place for all other policies and so in this way staff are updated as policies and guidance change.

The Online Safety Coordinator communicates to form teachers any online safety issues as and when they arrive as well as any information or updates that have come to light from Government guidance; advice can be sought at any time from the relevant member of the safeguarding team, Online Safety Coordinator or Assistant Head Academic.

Parents

Parents play an essential role in the education of their children and in the monitoring and regulation of their child's online behaviour.

Online safety information and awareness is provided to parents via email and the Pupil Acceptable Use Policy, which parents must acknowledge they have seen and discussed with their daughter. As well as this, school events such as parents' discussion evenings or forums are held throughout the year. The Online Safety Coordinator and Designated Safeguarding Lead organise parent talks from external parties on a range of topics relevant to the parent community. Any relevant information in regards to specific technology usage is relayed to parents as and when issues arise.

APPENDIX 1: St Christopher's Pupil Acceptable Use Agreements

Online Safety Acceptable Use Agreement (Reception – Year 2)

I agree that my daughter will abide by the following rules when using computers and other digital devices both in and out of school.

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

- Ask a teacher or adult for permission before using them.
- Only use websites or apps that a teacher or trusted adult has told me to or allowed me to use.
- Tell my teacher immediately if:
    - I click on a website by mistake;
    - I receive messages from people I don't know;
    - I find anything that may upset or harm me or my friends.
- Use school computers for schoolwork only.
- Be kind to others online and not upset them or be rude to them online.
- Look after the school IT equipment and tell a teacher straight away if something is broken or not working properly.
- Only use the username and password I have been given.

- Try my hardest to remember my username and password.
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of a trusted adult.
- Save my work on the school network or through OneDrive when instructed to do so.
- Log off a computer when I have finished using it.
- Never bring files or devices into school without permission (including phones, iPods, tablets, USBs, E-readers, smartwatches, Fitbits, smartphones, and cameras).

Online Safety Acceptable Use Agreement (Year 3 – Year 6)

I agree that my daughter will abide by the following rules when using computers and other digital devices both in and out of school.

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

- Use the school's computers for school-related purposes only.
- Use OneDrive and Teams for school-related purposes only.

- Use Canva for school-related purposes only.
- Never bring files or devices into school without permission (including phones, iPods, tablets, USBs, E-readers, smartwatches, Fitbits, smartphones, and cameras).
- Ask for permission from a staff member before using my device and the Internet; not visit unrelated sites/apps.
- Ask permission before looking at other people's files.
- Delete only my own files (on OneDrive, Canva etc).
- Ensure that any comments I make anywhere online at school or home are polite, sensible, and appropriate to the task.
- Share documents (on OneDrive, Canva etc) with my peers and teachers only when a teacher has given me permission)
- Adhere to academic honesty and avoid plagiarism.
- Refrain from being friends with staff members on social networking sites and from contacting them via email.
- Avoid contacting anyone online whom I do not know on any app or website. If someone contacts me, I will inform a trusted adult immediately.
- Communicate through relevant school channels only.
- Communicate kindly online and keep in mind that my digital footprint is permanent.
- Exercise caution when opening links or downloading files and trust only known sources.
- Never share my personal information (home address, phone number, photos etc.) unless a trusted adult permits sharing.
- Keep my passwords for my digital devices and online platforms confidential.
- Seek permission and take a trusted adult when arranging to meet someone I've only interacted with online.
- Avoid using generative AI tools such as image and text generators on any website or app unless I have permission from a trusted adult because I know that I need to be 13 years old to do so.
- Understand that teachers regularly monitor the use of my device using SENSO and that anything I do online can be traced back to me, regardless of whether I delete it or not.
- Report any concerning messages or content I see online to a parent or teacher immediately.
- Respect age restrictions on websites and apps. I understand that lying about my age is inappropriate. I will discuss any such situations with my parent/guardian/teacher.
- Maintain respectful online behaviour both in and out of school to avoid distress or harm.
- Recognise that online actions have real-world consequences affecting others.
- Acknowledge that these rules aim to keep everyone safe and that failure to follow them may result in sanctions, including removal of access to my device or the school network for a period, or an investigation.

Year 6 only:

- Understand that bringing a mobile phone to school for safety requires me to hand it to the office before/during form time and then pick it up at the end of school.

Any breach of these rules will be dealt with in accordance with the school behaviour policy and may lead to sanctions, including the withdrawal of access to the school network and/or further consequences.

APPENDIX 2: Acceptable Use Agreement for Staff, Volunteers, and Governors

To be used in conjunction with the Acceptable Use Policy for staff.

When using the school's IT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms for personal and non-professional use
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with the Designated Safeguarding Lead / the Head first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor my device and the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and Head of IT know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will only use the school's IT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I understand that the school encourages minimal personal use of school devices; however, within reason and where necessary I may use a school device for personal reasons (i.e. checking emails).

I understand that my social media profiles should not be accessible to pupils. If I have a personal profile, I will use a first and middle name and set it to private. Exceptions apply to staff with public professional interests, who will ensure the content they post is appropriate for the school community

APPENDIX 3: Information for parents

At Home

At home, it is important that parents and carers continue to reinforce the messages learned in school. For this reason, parents are being asked to review our updated Pupils Acceptable Use Policy. Please take the time to discuss the contents of the AUP with your daughter to ensure she fully understands the key points.

At home we strongly recommend:

- That you keep open lines of communication between you and your child to support their use of technology and specifically the internet.
- That any device your child uses at home are in family rooms (rather than in children's bedrooms) with the screen in view.
- That you install monitoring and filtering software to block access to inappropriate content (these types of software can be purchased from any IT store.)
- That a family email address is used, rather than children having their own private email addresses.
- That you do not allow your children to access the internet on mobile phones and portable devices.
- That you monitor the amount of time your child spends online.

- That you discourage the use of social networking sites under the age of 13 and adhere to age restrictions: The minimum age to open an account on Facebook, Twitter, Instagram, Tik-Tok and Snapchat is 13. WhatsApp has a minimum age of 16. YouTube requires account holders to be 18 unless with parent consent which then is 13.

Parents are expected to ensure that internet access and social media usage through personal devices and mobile contracts is appropriate to their daughter's age. Parents should also be responsible for giving guidelines to their daughter about the amount of time spent using their devices.

Whilst the school takes the actions described above to ensure that students understand the importance of safe behaviour online, the school cannot be held responsible for inappropriate online behaviour that bypasses the school network.

In light of this, parents must also be responsible for ensuring that their daughter uses technology in a safe and secure way and behaves responsibly when online. The full range of school sanctions will be considered in the event of any breach of this code of conduct or the school's Behaviour Policy.

Both the school and parents have a responsibility to ensure that students have the knowledge and confidence to know what to do if they encounter content or receive communications that make them feel uncomfortable, worried or upset and are able to share their concerns in an open and supportive environment.

A Guide to Internet Security for Parents

There is no fool-proof method of protecting children from harmful content on the internet. A discussion with your child about the risks of using the internet and how to avoid them is a key component of any child protection approach. www.childnet.com has helpful suggestions on all aspects of protecting children on the Internet.

There are many different levels of parental controls ranging from blocking certain sites to full scale spyware which allows you to see everything your child is doing on their device. You will have to decide what devices you would like to protect, which environments you want to protect and the level of restriction you want to place on your children.

There are 3 ways that your children can connect to the internet:

1) Your home Broadband, which will generally also provide WiFi to your house. Any device including your PC, which connects to your home WiFi can be protected by the parental controls offered by your Broadband provider. Most of the UK Broadband market is supplied by BT, Sky, Talk Talk or Virgin, who all offer various forms of protection if you request it. In addition, you can buy parental control software (such as AVG Family Safety, McAfee Family Protection, Bsecure Online and Webwatcher) from a number of suppliers which will also secure your home environment and in some cases your children's devices.

2) Your mobile network operator. Any device with a mobile SIM can access the internet through the mobile network – including at home. The major mobile operators protect network users by enabling you to block inappropriate content in accordance with BBFC categories. You can only lift this block if you can prove you are over 18. Vodafone provides an app for Android smartphones called "Vodafone Guardian" which offers further protection.

3) Public WiFi can be accessed in various ways and from various sources by almost any modern smartphone, tablet or laptop. It is the hardest environment to control and the only way for parents to protect children in this environment is to install parental control software on the device itself. Parental control software can be found in the Apple App store or in Google Play. You will need to download the program that suits you best.

APPENDIX 4: Information and Support

- Teaching online safety in schools - DfE guidance outlining how schools can ensure their pupils

understand how to stay safe and behave online as part of existing curriculum requirements.

- Keeping Children Safe in Education - Statutory guidance for schools and colleges on safeguarding children and safer recruitment.

Childnet	https://www.childnet.com/	Offers information for parents and teachers on online safety
Digizen	https://www.digizen.org/	Focus on digital citizenship and what it means to be part of the online community
Think you know	https://www.thinkuknow.co.uk/	CEOP programme accessible to teachers and parents providing information on a range of online safety issues
Net Aware	https://www.net-aware.org.uk/	Useful site providing information on a range of websites, games and apps that children have access to
Internet Matters	https://www.internetmatters.org/	Aimed at parents to support keeping their children safe online
UK safer internet centre	https://www.saferinternet.org.uk/	Resources available to both parents and teachers
Common Sense Media	https://www.commonsensemedia.org/	Resources and information for parents and educators on a range of popular apps and games

APPENDIX 5: Remote education

Remote education is likely to increase online safety issues and therefore raises its importance.

When pupils need to be educated remotely, they will be provided information directly by form teachers during form times through class discussions. This will include support that enables girls to know what warrants a concern in terms of their safety online and how to report it. It will also include reference to child-on-child abuse (see the Anti-bullying Policy). Pupils will also be reminded that although they are working remotely, the Acceptable Use Policy is still in place and they should consider this at all times when working on devices or online.

Staff members are required to follow the protocols outlined in the Staff Code of Conduct and the Acceptable Use Agreement.