E-Safety Policy

Person responsible	DSL/E-Safety Coordinator
Last update	September 2023
Frequency of Review	Annually
Date of next review by Governors	Autumn 2025

Contents

1. Introduction and overview

1.1 Rationale

This policy sets out St Christopher's The Hall's ("the School") intentions and aims to safeguard children in relation to the online world. It was created in response to delivering the expectations of KCSIE 2023. The aim of the policy is that children should not be able to access harmful or inappropriate material from the school or colleges IT system and that "over-blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding. Appropriate filters and monitoring systems are in place and maintained, with the DSL having responsibility for understanding the filtering and monitoring systems and processes in place as part of their remit.

It also forms part of the requirement in the School's Prevent Duty "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"

This E-Safety Policy is part of the School's Safeguarding remit. This policy relates to other policies including: the Code of Conduct for Staff, Anti-Bullying, Child Protection, Social Media Policy and the Acceptable Usage Policies. The policy has been developed in light of a review of the School's safeguarding practice in the use of technology and its benefits and risks and the increased prevalence of technology in the classroom. Staff, parents, carers and pupils themselves are involved in deciding the policy. The School believes that it provides a caring, positive, safe and stimulating environment where children can develop.

The School fully recognises the responsibility it has to the safeguarding and protection of pupils who use our service. All staff members, including volunteers, have a full and active part to play in protecting children and pupils from harm. This policy is also to be used in conjunction with online home teaching by the School e.g. Google Classroom.

This policy should cover the responsibility of the School to safeguard children from harm, responding to and investigating incidents, protecting staff, and storing information securely.

1.2 Aims

- Ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupils or liability to the School.

- Raise awareness and understanding of E-Safety issues amongst children and pupils where they are using the School's equipment.

- Support and encourage the pupils to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.

- Support and encourage parents and carers to do what they can to keep their children safe online.

- Ensure that staff understand the importance of E-Safety in safeguarding and develop their understanding of the signs and indicators of abuse.

- Ensure that all members of staff are aware of actions required to assist a child or young person who reports e-abuse or other online concerns.

- Ensure staff know how to respond to a young person who discloses abuse.

- Establish safe access to the internet for pupils.

- Provide a systematic means of monitoring children known or thought to be at risk of harm.

- Ensure that all adults who have access to children's information have been checked as to their suitability and have an enhanced DBS and barred list check, as well as online searches carried out during recruitment.

- Develop an online safety agreement for use with pupils and their parents/carers.(Acceptable Use Policy)

- Develop clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.

1.3 Roles and responsibilities

Roles and responsibilities

Role	Key Responsibilities
Head and DSL	To take overall responsibility for E-Safety provision To ensure the School uses an approved, filtered internet service, which complies with current statutory requirements To be responsible for ensuring that staff receive suitable training to carry out their E-Safety roles and to train other colleagues, as relevant To be aware of procedures to be followed in the event of a serious E-Safety incident To have regular monitoring meetings with safeguarding team (which includes the ESafety Coordinator) The DSL has responsibility for understanding the filtering and monitoring systems and processes in place as part of their remit.
Bursar	To take overall responsibility for data and data security
E-Safety Coordinator	Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the School E-Safety Policy Promotes an awareness and commitment to E-Safeguarding throughout the school community Ensures that E-Safety education is embedded across the curriculum Liaise with school ICT/Computing technical staff Communicates regularly with SLT and the designated Safeguarding Governor to discuss current issues and review incident logs To ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident To ensure that the E-Safety incident log is kept up to date by monitoring the traffic through the School's filtering systems. Facilitates training and advice for all staff Is regularly updated in E-Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:

	• sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media
Governors	To ensure that the School follows all current E-Safety advice to keep the children and staff safe To approve the E-Safety Policy and review the effectiveness of the policy To support the School in encouraging parents and the wider community to become engaged in E-Safety activities The role of the Governor/s will include regular review with the DSL/E Safety Coordinator (including E-Safety incident logs)
Teachers of Computing	To oversee the delivery of the E-Safety element of the Computing curriculum To liaise with the E-Safety Coordinator regularly
IT Systems Manager	To report any E-Safety related issues that arise, to the DSL To ensure that provision exists for virus and security threats (e.g. keeping virus protection up to date) To ensure the security of the School ICT system To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices Ensures the School's policy on web filtering is applied and updated on a regular basis Keeps up to date with the School's E-Safety Policy and technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant The use of the School network/website/remote access/email is regularly monitored in order that any misuse or attempted misuse can be reported to the DSL or Head for investigation

	To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster Keep up-to-date documentation of the School's E-Security and technical procedures Ensure that all data held on pupils is adequately protected
All Teachers	To embed E-Safety issues in all aspects of the curriculum and other school activities To supervise and guide pupils carefully when engaged in learning activities involving online technology, including, extra-curricular activities if relevant Ensure that pupils who bring mobile phones to school have handed them in to the office on arrival and, if necessary routinely check, this is the case, ensuring phones are sent to the office if they are seen out or are being used.
All Staff	To read, understand and help promote the School's E-Safety Policy and guidance To read, understand, sign and adhere to the School's staff Acceptable Use Policy as stated in the E-Safety policy To be aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement the School's policies with regard to these devices To report any suspected misuse or problem to the E-Safety Coordinator Consult with the School if they have any concerns about the children's use of technology
External groups	Any external individual/organisation will sign an Acceptable Use Policy prior to using any equipment

1.4 How the policy will be communicated to staff/pupils/community

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the School website and saved on the shared cloud area
- Policy to be part of the School induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable Use Policy to be issued and signed by whole School community, yearly

- Acceptable use agreements to be held in the case of pupils by the Computing teacher and for adults in personnel files
- E-Safety is part of the Safeguarding Booklet, given to visitors, outlining the School's expectations.

1.5 Handling complaints

The School will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The School cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include but are not limited to:

- Interview/counselling by class teacher/Head of Phase/E-Safety Coordinator/DSL/Head;
- Informing parents or carers;
- Removal of internet or computer access for a period, [which could ultimately prevent access to files held on the system]
- Referral to Police.

The DSL or E-Safety Coordinator act as the first points of contact for any complaint. Any complaint about staff misuse is referred to the Head.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with our Child Protection and Safeguarding Policy.

Complaints relating to external users, such as extracurricular club providers will be followed up using the existing policies and procedures. These will be referred to the DSL and Head, and may include informing the LADO.

2. Child Protection On-line

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, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: child on child 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: 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; and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The School ensures online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the Designated Safeguarding Lead and any parental engagement.

The School recognises the view made in the previous document KCSIE 2022 that "Many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G)." and that this may lead to unsafe or in some cases illegal activities. The School aims to mitigate this by the removal of all mobile phones from children where children bring them to school at the point of entry. Personal devices are not allowed on the premises and are confiscated when found. These devices are returned in accordance with the detail in the Devices section of this policy.

3. Education and Curriculum

3.1 Pupil E-Safety Curriculum

All pupils need to learn to evaluate everything they read, hear and view and to refine their own communications with others via the Internet.

- Pupils will be advised on what Internet use is acceptable, what is not and given clear objectives for Internet use – Acceptable Use Policy rules are given out to every new child, plus existing pupils annually. They are to sign and return the Acceptable Use Policy to be held on file.
- Internet access will be planned to enrich and extend learning activities.
- Access levels will be reviewed to reflect the project requirements and pupil's age.
- Staff should be available to provide guidance. Children will not be able to access the Internet unsupervised.

Pupils should be helped to understand what to do if they experience material that they find distasteful, uncomfortable or threatening, and this is part of their computing curriculum as well as being reinforced in the broader curriculum.

Children and staff need to know how to deal with any Cyber Bullying incidents.
Pupils need to know about the national agencies, such as Child Exploitation Online Protection (CEOP), http://www.ceop.gov.uk/ – so that in an extreme case, they know how to "report abuse".

In Reception to Year 2 children are taught:

-What to do and who to tell when they see something inappropriate online.

-What is personal information and why we should not give it out to strangers.

-How to treat people online.

In Year 3 to Year 6 children are taught the above in more depth and focus on the following:

-Understanding what is on the internet stays there indefinitely and the possible consequences.

-Mobile phone and social media safety.

Fraud and hacking.

Introduction to 'fake news' and how to combat it.

Online safety to include grooming, radicalisation and social media use.

3.2 Remote Learning

Where children are being asked to learn online at home the Department of Education has provided advice to support schools and do so safely: Safeguarding and remote education during coronavirus (COVID-19) - GOV.UK Reference to this is also made in the Acceptable Use Policies for pupils and for staff.

3.3 Staff and governor training

All staff and Governors should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

Staff receive this as part of their induction and are regularly updated.

In the School:

Where needs have been identified in this area the E-Safety Lead and DSL will source and deliver necessary training. This may be provided directly or from an external

agency.

3.4 Parent awareness and training

In the School, this will take the form of:
Visits from NSPCC or other organisations, who deal with online safety and bullying in workshops appropriate for the key stage.

Use of a formal Wellbeing programme linked in with a strong PSHE curriculum (JIGSAW)

A filtering system (Smoothwall) on all computers used regularly by children, which is creating an incident log which can be reviewed and shared with parents if necessary

Regular discussions and planned lessons for children on internet safety with the teacher(s) of Computing

4. Incident management

4.1 Filtering and monitoring

All Staff need to safeguard and promote the welfare of children and provide them with a safe environment in which to learn and should be doing all that they reasonably can to limit children's exposure to the above risks from the School's IT system. The filters and monitoring systems in place are part of the Smoothwall system which can create reports on infringements of preset and user defined parameters, including, but not limited to, specific words/phrases being typed or websites being accessed. The E-Safety coordinator has responsibility for monitoring these systems.

4.2 How will information systems security be maintained?

The security of the School's information systems will be reviewed constantly and in relation to any E-safety related events that occur. Virus protection will be updated regularly.

- Personal data sent over the Internet will be encrypted or otherwise secured.
- Personal data, other than progress reports currently being prepared by and relevant to staff, should not be held on portable media without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in work areas or attached to email.
- Files held on the organisation's network will be regularly checked.

- Filtering systems will be regularly maintained.

4.3 User policies

The School:

- Will provide guidance on users acting reasonably;
- Requires all staff and pupils to sign an Acceptable Use Policy agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search; and uses "cleaning tools" such as View Pure when watching internet video sources such as YouTube.
- Informs users that Internet use is monitored;
- Informs staff and pupils that they must report any failure of the filtering systems directly to the systems administrator and/or SLT and E-Safety Lead.
- Ensures that our systems administrators report to SLT where necessary;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the data collection permission form sent out to parents at the point of entry, and subsequently every year.
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material suspected to be illegal to the appropriate authorities – Police – and the Local Authority.

4.4 Publishing material

The use of images and taking of video or photographs of pupils requires parent/carer consent.

Pupils need to be made aware of the reasons for caution in publishing personal information and images in social publishing sites, and are taught through the curriculum about keeping this information safe.

A data collection form will go out each year and asks parents to identify specific consents for various use of images of the pupils in relation to the School social media and website or advertising and newsletters. This also includes pupils' work.

4.5 Tips for keeping safe online:

- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging and email addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the child or his/her location e.g. house number, street name or school.
- Staff official blogs or wikis should be password protected and run from the school website. Staff should be advised not to run social network spaces for pupils's use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others.
- Pupils should be advised not to publish specific and detailed private thoughts.
- The School is aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments.
- Staff social media profiles should be set to private and not searchable by others. Avoid using your actual name in your profile.
- Staff should not be "friends/following" etc any current parent of children at the school, or contacting them via social media platforms.
- An adult connected to the School should not have contact with any current pupil outside of approved systems such as Google Classroom.
- An adult connected to the School should not have contact with any former pupil under the age of 18.
- Items connected to pupils such as their work should not be posted to social media or shared outside the classroom, even in anonymised forms.
- It is strongly recommended that staff who are also parents do not join class WhatsApp groups.
- It is also strongly recommended that staff maintain a pattern of observance-only on platforms such as Beckenham Appreciation Group and similar, and

refrain from commenting on the opinions given so that they are not associated with the School.

4.6 Protecting Personal Data

The Data Protection Act 2018 ("the Act") gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly and works alongside the General Data Protection Regulation (GDPR).
The Data Protection Principles from the Act and the GDPR that are used in the School are that personal data must be:

- Used fairly, lawfully and transparently;
- Used for specified, explicit purposes;
- Used in a way that is adequate, relevant and limited to only what is necessary;
- Accurate and where necessary, kept up-to-date;
- Kept for no longer than is necessary;
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage;

The Act allows for stronger legal protection for more sensitive information such as health, religious beliefs, race ethnic background etc.

- Staff must immediately tell the Headteacher or the Bursar if they become aware of anything which might mean that there has been a data protection or security breach.
- This could be anything which puts personal data at risk, for example: if personal data has been or is at risk of being destroyed, altered, disclosed or accessed without authorisation, lost or stolen.

In the case of not being able to contact the Headteacher or Bursar, contact your head of phase or E-Safety Lead.

All of the following are examples of a security breach, but are not exhaustive.

- You accidently send an email to the wrong recipient
- You cannot find or have misplaced papers which contain personal data
- Any device (such as a laptop or a smartphone) used to access or store personal data has been lost or stolen or you suspect that the security of a device has been compromised

In certain situations, the School must report an information security breach to the Information Commissioner's Office (the data protection regulator) and let those whose information has been compromised know within strict timescales. This is

another reason why it is vital that you report breaches immediately and give as much information as you can.

An overview of the investigative procedure carried out by the school on each incident is given in appendix B of this policy.

5. Managing the ICT infrastructure

The School has a dedicated role of IT Systems Manager to provide the maintenance of systems and processes, which is listed above in the responsibilities part of this policy.

5.1 Devices.

5.1.1 General guidance:

Devices issued by the School will be encrypted, monitored and remain the property of the school. This includes laptops and class computers. Mobile devices such as school iPads and school issued mobile phones will be passcode/password protected and similarly monitored.

Avoid common problems:

- **Lock computer screens**: Staff computer screens should be locked when not in use, even if they are only away from the computer for a short period of time. To lock your computer screen press the "Windows" key in addition to the "L" key. If you are not sure how to do this then speak to the IT Manager or E-Safety Lead. Computers are configured to automatically lock if not used for a period of thirty minutes.
- **Be familiar with your IT**: Staff should familiarise themselves with any software or hardware that they use. In particular, they should understand what the software is supposed to be used for and any risks. For example: a "virtual classroom" such as Google Classroom which allows lesson plans and exam papers for pupils to be uploaded need care to ensure that anything more confidential is not accidently uploaded or disclosed.
- **Know how to properly use any security features.** Extra care needs to be taken about where information containing personal data is stored. For example, safeguarding information should not be saved on a shared computer drive accessible to all staff. Encrypt any personal data being sent to another. If in doubt, speak to the IT Manager
- **Hardware and software not provided by the School must not be used without permission**. Software, apps or programmes should not be downloaded or installed without permission from the IT Manager. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to school systems without permission.
- School documents should not be shared on private cloud storage or file sharing accounts

- **Portable media devices:** The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed unless those devices have been given to you by the IT Manager (see also point 4.2). The IT Department will protect any portable media device given to you with encryption
- **Documents containing personal data must not be worked on by staff whilst travelling if there is a risk of unauthorised disclosure** (for example, if there is a risk that someone else will be able to see what you are doing). For example, if working on a laptop on a train, you should ensure that no one else can see the laptop screen and you should not leave any device unattended where there is a risk that it might be taken.
- **Appropriate security measures should always be taken.** This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date.
- All school documents (including school emails), and any software applications provided for school purposes, must be removed from any personal device if a staff member ceases using a device for school work, or if you are about to leave the School. If this cannot be achieved remotely, the device must be submitted to the IT Department for wiping and software removal.

5.1.2 Personal Devices:

- Mobile phones and personally-owned mobile devices brought into the School are entirely at the staff member, pupil's & parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into the School
- Visitors to the School are expressly asked not to use their mobile devices while in the School premises, and compliance with this request is monitored by staff.
- The School reserves the right to search the content of any mobile or handheld devices on the School premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- The recording, taking and sharing of images, video and audio on any mobile phone is prohibited; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded.
- All mobile phone use is open to scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time if it is deemed necessary.
- Mobile phones and personally-owned devices approved for use by the Headteacher in exceptional circumstances are not permitted to be used in certain areas within the School e.g. changing rooms and toilets.
- Staff members may use their phones during school break times in certain areas. They should be switched off or silent at all times, when not in use.

- Staff are not permitted to use their own mobile phones or devices for contacting pupils or their families within or outside the School in a professional capacity.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose. If the need is necessitated, then the photos must immediately be wiped when the photos are transferred to the Google Shared Drive.
- If a member of staff breaches the School's E-Safety policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for School duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, they should use one of the School owned devices. In situations where this is not possible they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- All visitors are requested to keep their phones on silent and out of sight.
- Where parents or pupils need to contact each other during the school day, they should do so only through the School Office/Head's PA.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- The School strongly advises that pupil mobile phones should not be brought into School. However, the School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. Where agreement has been made for a mobile device to be brought to the School by a pupil, mobile phones are handed into the School Administrator on arrival at school, logged and handed back at the point at which the child leaves for the day.
- If a pupil breaches the School Policy then the phone or device will be confiscated and will be held in a secure place in the School office. Confiscated devices will be released to parents or carers once the breach has been discussed and resolved.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences during curriculum provision.

5.2 Passwords

- Passwords should be long and difficult to guess, for example, use a song lyric or a memorable phrase plus a number

- Do not choose a password which is so complex that it's difficult to remember without writing it down
- Passwords should not be disclosed to anyone else
- Passwords which other people might guess or know, or be able to find out, such as your address or your birthday, should not be used
- A password which is used for another account must not be used. For example, you must not use your password for your private email address or online services for any School account
- Passwords (and any other security credential you are issued with such as an encryption code) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down

5.3 E-mail

- When sending emails care must be taken to make sure that the recipients are correct.
- When sending emails to multiple recipients Cc must be used when you want to copy others publicly, and Bcc when you want to do it privately. Any recipients on the Bcc line of an email are not visible to others on the email. This avoids potential information breaches by disclosing other's email addresses
- If the email contains critical personal data then you should ask another member of staff to double check that you have entered the email address correctly before pressing send.
- Encryption: Remember to encrypt internal and external emails which contain personal data. For example, Microsoft Office documents can be attached to email and encrypted with a password. This password can then be forwarded separately to the recipient.
- Private email addresses: You must not use a private email address for any School related communication. You must only use your School address. Please note that Governors may need to use their personal email addresses.

5.4 Printing:

- When printing documents, especially email, collect everything from the printer straight away, otherwise there is a risk that confidential information might be read or picked up by someone else.
- If you see anything left by the printer which contains personal data then you must hand it in to the Bursar

5.5 School website

- The school website and social media pages remain the property of the School.
- Provision of materials on these pages is done by a few individuals who have been granted access by unique credentials. These credentials provide hierarchical levels of permissions to different areas and enable the content to be changed.

- These access arrangements are subject to change should the need arise, and are not to be shared with others.

Within the website will be a "report abuse" functionality, feeding back to the E-Safety Lead, which will form part of the regular review of the Incident Log.

5.6 Social Media (see also points 4.4 & 4.5 plus the Social Media Policy)

- The School defines social media as 'any websites and applications that enable users to create and share content or to participate in social networking'.
- Social networking sites and tools include, but are not limited to, Facebook, Twitter, Snapchat, TikTok, LinkedIn, MySpace, Flickr, YouTube and Instagram. It also includes forums and discussion boards such as Yahoo! Groups or Google Groups, online encyclopaedias such as Wikipedia, and any other web sites which allow individual users or organisations to use simple publishing tools.
- All members of the School should bear in mind that information they share through social networking applications, even if they are in private spaces, may be subject to copyright, safeguarding and data protection legislation.
- Social media is an increasingly influential part of life particularly for pupils. It has been identified as an important tool in the sharing of extreme material and extremist groups are actively using social media to inform, share propaganda, radicalise and recruit for their cause.
- Social media safeguarding is an important element of protecting pupils from extremist narratives and *Prevent* can play an active part in this process.

In the School:

- Social networking sites will be blocked using suitable filtering systems to block inappropriate content, including extremist content where possible.
- Parents and pupils will be provided with information on the safe use of the internet, through assemblies, workshops, talks and regular publications.
- Where staff, students or visitors find unblocked extremist content they must report it to the Designated Safeguarding Lead or in their absence, a senior member of staff.
- The School will own and manage social media accounts by specific named people who have access via unique credentials.
- The content of any School-sanctioned social media site and/or social media accounts should be entirely professional and should reflect well on the School.
- No member of staff should create a social media account linked to the School for any purpose, this also applies to other virtual environments, such as online gaming.
- Any unauthorised accounts linked to or pertaining to be official School accounts should be reported immediately to the Headteacher, IT Manager or E-Safety Lead.

- Any links to external sites from the accounts must be appropriate and safe; if they are shared these must be verified as reputable sites.
- Only appropriate hashtags should ever be used.
- Any inappropriate comments on, or abuse of, School-sanctioned social media and/or social media accounts using the name of the School, its logo, or clearly attached to the School in some way, should immediately be removed and reported to the E-safety Officer, DSL and the Headteacher where appropriate, and should form part of the review of reported incidents.
- Any communication received from current pupils on any personal social media sites must be reported immediately to the DSL and to the E-Safety Officer.
- If any member of staff is aware of any inappropriate communications involving any student in any social media, these must immediately be reported to the DSL and to the E-Safety Lead and will form part of the review of the incident log.
- Staff should not post or publish on the internet or on any social networking site, any reference to the School, their colleagues, parents or pupils or discuss pupils or colleagues or criticise the School or staff.
- Staff may like, share or make appropriate comments in response to the School's official social media accounts.
- Staff are strongly advised to consider the reputation of the School in any posts or comments related to the School on any social media accounts.

Social Media and Privacy Law

Social networking sites are inherently insecure places to have discussions which may contain sensitive information. Privacy laws can be violated and the reputation of the School can be damaged if the public sees a discussion of any sensitive information taking place on social networking.

Staff should be aware that these types of cases can result in disciplinary action.

Proprietary Information:

- Staff may not share information which is confidential and proprietary about the School.
- This includes information about services, programmes, financial, strategy, and any other internal confidential, proprietary, or sensitive workplace information that has not been publicly released by the School.
- These are given as examples only and do not cover the range of what the School considers confidential and proprietary.
- The School respects staff member rights to privacy and to express themselves. However, the School and staff members must also respect, and diligently protect, the privacy of fellow staff members, pupils, parents, and others.
- Privacy and confidentiality must be maintained in every possible way. Staff must not discuss pupil or family related information via social networking and

public social media, texting, or online unless it is an approved medium and for a School related purpose.

- Staff are advised to be extremely cautious in conversations with other staff, parents and volunteers in social networking, on the basis that privacy laws can be violated even if a person's name is not shared.
- The School will honour the privacy rights of current and past employees, current and past pupils and their families, and anyone else associated with the School, by seeking permission before writing about or displaying internal School happenings which might be considered to be a breach of their privacy and confidentiality.
- Staff must understand that on-line content is difficult, if not impossible to retract once posted or sent.
- Staff should recognise that there is the possibility of being legally liable for something inappropriate which is shared online.
- Any concerns or issues about the School, its pupils or staff should be expressed directly to the School and not be voiced on social media.

Parents and Social Media

- Parents must obtain permission before posting pictures that contain other parents or their children, unless sharing or liking a post from the School's official social media account.
- If parents become aware of inappropriate use of social media by their own or other people's children, they should contact the School so that the School can work with the parents to educate pupils on safe and appropriate behaviour.
- If parents become aware of the inappropriate use of social media by other parents or staff, they should inform the School so that steps can be taken to remedy the situation.
- Parents' are allowed to take photos or videos of their children at school events for their own personal use. They must not upload them onto social media sites (if they have other children in them), without the permission of that child's parents.

Other visitors to the School (e.g. theatre groups or workshop providers) are not to photograph or film pupils during a school activity without the parents' permission.

5.6 Video conferencing

Some recognised threats to Video conferencing are:.

- Threats to privacy, identification, or Personally Identifiable Information
- Risks to data from data theft or breaches.
- Risks to confidential business or corporate information or intellectual property.
- Meeting hijackings.
- Access to confidential meeting recordings.

In the School:

- Google Meet is used to make contact with pupils. No personal devices are to be used for this and no images or recordings are to be made on personal devices.
- The Google Meets will be recorded for safeguarding purposes and this is stored securely in Google Drive.

Guidelines for keeping video conferences safe:

- Keep Invites Private

Do not share meeting invites/codes outside of Google Classroom when meeting a class online. For other types of online meeting, do not share the access credentials on social media or take screenshots of the link to pass around. It's best to email the link directly from the software or set up an invite in your email calendar.

- Don't Use Your Personal Meeting ID or the same meeting code every time.

Whilst it may be tempting to copy your Personal Meeting ID and use that for every meeting, it also means that if someone gets hold of the link they can drop in and disrupt things whenever they like, so it's always advisable to set up a unique ID for every meeting. Google Meet uses a unique code which can be changed and sent to the class each time. (Instructions for this are in the staff guide to using Google Classroom)

- Require a Password

Ensure your meetings are protected by a password and share that password as part of the invitation. Having a different password for every single meeting will help protect against hackers.

- Turn Off Screen Sharing

Turn off screen sharing. If a hacker does get into your system they're then able to share with everyone in the meeting what's up on your screen – so if you've been looking at your online banking 5 minutes before you can see where there might be a problem.

6 The Prevent Duty (see also Safeguarding Policy)

- The School ensures that children are safe, as far as possible, from terrorist, extremist and radicalisation material when accessing the internet in School.
- Suitable filtering is in place to ensure that children are safe from terrorist, extremist and radicalisation material when accessing the internet in School.
- Pupils' will be equipped to stay safe online, both in School and outside of School.
- Internet safety will be integral to the School's Computing curriculum and is also embedded in PSHE and RE.
- All staff are aware of the risks posed by online activity of extremist and terrorist groups, and know how to deal with it accordingly.

- Arrangements to respond to pupils who may be targeted or influenced to participate in radicalism or extremism is of a high priority.
- The Acceptable Use Policy (AUP) for staff, pupils and parents, and visitors, refers to preventing radicalisation and related extremist content.
- To report any online terrorist related material visit: www.gov.uk/report-terrorism (see **Child Protection Policy** for more details)

Appendix A – Keeping Children Safe in Education 2023

Extract from KCSIE (SEPT 2023) concerning online safety:

Online safety
135. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

136. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk: content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism. 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 37 UK Council for Internet Safety Education subgroup is made up of sector experts who collaborate to produce advice and guidance to support schools and colleges keep their children safe online. 38 Public Health England: has now been replaced by the UK Health Security Agency and the Office for Health Improvement and Disparities (OHID), which is part of the Department of Health and Social Care, and by the UK Health Security Agency, however branding remains unchanged. 36 purposes. conduct: 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, and commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

137. Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement. Online safety policy

138. Online safety and the school or college's approach to it should be reflected in the child protection policy which, amongst other things, should include appropriate filtering and monitoring on school devices and school networks. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college

should have a clear policy on the use of mobile and smart technology, which will also reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

The full version of Annex B of the KCSIE 2023 also explains other information and resources that children and parents may refer to. This is a list of resources that are searchable, however their links can be found here: Keeping children safe in education 2023

Additional advice and support: There is a wealth of information available to support schools and colleges. The following list is not exhaustive but should provide a useful starting point:

Online safety-advice

Childnet provide guidance for schools on cyberbullying

Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation

London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

NSPCC E-safety for schools provides advice, templates, and tools on all aspects of a school or college's online safety arrangements

Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective

Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones

South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

Online Safety Audit Tool from UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring

Online safety guidance if you own or manage an online platform DCMS advice

A business guide for protecting children on your online platform DCMS advice

UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Online safety- Remote education, virtual lessons and live streaming

Case studies for schools to learn from each other Guidance Get help with remote education resources and support for teachers and school leaders on educating pupils and students

Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely

London Grid for Learning guidance, including platform specific advice

National cyber security centre guidance on choosing, configuring and deploying video conferencing

UK Safer Internet Centre guidance on safe remote learning

Online Safety- Support for children

Childline for free and confidential advice

UK Safer Internet Centre to report and remove harmful online content

CEOP for advice on making a report about online abuse

Online safety- Parental support

Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support

Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents

Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world

How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online

Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation

London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games

Parentzone provides help for parents and carers on how to keep their children safe online

Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parent guide on talking to your children about online sexual harassment

#Ask the awkward – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships.

Appendix B - Investigative procedure to be followed for each incident.