Online Safety Policy

Person responsible	**Assistant Head Pastoral (Online Safety Coordinator)**
Last update	**October 2025**
Frequency of Review	**Annual**
Date of last review by Governors	**November 2025**
Date of next review by Governors	**November 2026**

Contents

1. Introduction and Aims

The main aims of the Online Safety Policy at Bute House Preparatory School (the School) are:

- To promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which empowers the School to protect its community from potentially illegal, inappropriate and harmful content or contact
- To educate the whole school community about access to and use of technology
- To establish effective mechanisms in order to identify, intervene in and escalate concerns where appropriate
- To help promote a whole-school culture of openness, safety, equality and protection

This Policy forms part of the School's whole school approach to promoting child safeguarding and wellbeing, which involves everyone within the School and seeks to ensure the best interests of pupils, and is at the forefront of all decisions, systems, processes and policies. This Policy applies to all members of the School (including staff, pupils, volunteers, parents/carers, visitors, community users, etc.) who have access to and are users of School Information and Computer Technology (ICT) systems, both in and out of the School.

This Policy should be referred to alongside the following guidance:

- The Statutory Framework for the EYFS
- Education and Skills Act 2008
- Children Act 1989
- Childcare Act 2006
- The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)
- The Equality Act 2010
- KCSIE 2025
- DfE Behaviour Guidance
- Teaching online safety in schools (DfE, June 2019)
- Harmful online challenges and online hoaxes (DfE, February 2021)
- Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Digital, Culture, Media & Sport (DfDCMS)
- UK Council for Internet Safety (UKCIS), December 2020
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (DfE, July 2025)

A brief definition of the following terms should add clarity and aid navigation of this Policy:

Governing Body – as the proprietor of the School.

Staff – this includes all those who work for, or on behalf of, the School, regardless of their employment status, including contractors, supply staff, volunteers and Governors.

SLT – this is the Senior Leadership Team of the School, comprising the Head, Senior Deputy Head, Deputy Head, Assistant Head, Director of Finance and Operations and Director of People and Development.

Technology - When considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing and exchanging information. These areas will be collectively referred to as 'technology' in this Policy.

The purpose of this Policy is to:

- Set out the key principles expected of all members of the school community at the School with respect to the use of ICT-based technologies.
- Safeguard and protect the pupils and staff of the School.
- Assist school staff working with pupils to work safely and responsibly with the internet and other communication technologies, and to monitor their own standards and practice.
- Set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross-referenced with other School Policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for the school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse
- Lifestyle websites, for example pro-anorexia / self-harm / suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content
- Misinformation, disinformation and conspiracy theories that may influence pupil wellbeing or safety
- Deepfake technology used to create misleading or harmful content
- AI-generated images of minors (including those of a sexual nature)

Contact

- Grooming

- Cyber-bullying in all forms
- Identity theft and sharing passwords
- AI chatbots creating false intimacy or providing harmful advice to vulnerable pupils

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Commerce

- Risks such as online gambling, inappropriate advertising, phishing and financial scams including sextortion.
- Gaming monetisation risks, including in-game purchases that may develop gambling-like behaviours.
- Cryptocurrency and investment scams targeting young people.

Ref: KCSIE 2025

The School will deal with incidents within the remit of this Policy and the associated Positive Behaviour and Anti-Bullying Policies. Where known, the School will inform parents of incidents of inappropriate online behaviour that take place out of school.

2. Roles and Responsibilities

The Governing Body has overall responsibility for all matters which are the subject of this Policy and is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils.

Role	Key Responsibilities
Governors	• To ensure that the School follows all current online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the Policy

Role	Key Responsibilities
	● To support the School in encouraging parents and the wider community to become engaged in online safety activities ● To have regular reviews with the Online Safety Coordinator (including online safety incident logs) ● To ensure that the School has appropriate filtering and monitoring systems in place and to regularly review their effectiveness in order to demonstrate they are doing all they reasonably can to limit pupils' exposure to risks. The School currently utilises Smoothwall for filtering and Senso for monitoring
Designated Safeguarding Lead	● To take overall responsibility for online safety provision as part of safeguarding and child protection ● To manage safeguarding incidents involving use of technology in the same way as other safeguarding matters in accordance with the Safeguarding (Child Protection) Policy and procedures. This includes protecting children from maltreatment both within and outside the home, including online as outlined in KCSIE 2025 ● To liaise with the Network Manager to monitor technology use and practice across the School and assess whether any improvements should be made to ensure the online safety and wellbeing of pupils ● 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 online safety roles and to train other colleagues, as relevant ● To oversee the work of the Online Safety Co-ordinator
Director of Finance and Operations	● To take overall responsibility for data and data security

Role	Key Responsibilities
Online Safety Coordinator	● To take day to day responsibility for online safety issues and have a leading role, alongside the DSL and Governors, in establishing and reviewing the School Online Safety Policy ● To promote an awareness and commitment to online safeguarding throughout the school community, both at home and in School ● To ensure that online safety education is embedded across the curriculum ● To work with the DSL to liaise with school ICT/Computing technical staff ● To communicate 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 online safety incident ● To ensure that the online safety incidents (including details of internet activity and sites visited), along with associated actions, are logged using the appropriate tags on CPOMs ● To carry out relevant risk assessments following online safety incidents or current issues, including any action taken in response and how effectiveness of provision is evaluated ● To facilitate training and advice for all staff ● Along with the DSL and Governors, to keep the Online Safety Policy up to date and compliant with the law and best practice in online safety issues, and be aware of the potential for serious child protection issues that 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 ▪ use of AI and emerging technologies
Head of Computing	● To oversee the delivery of the online safety element of the Computing curriculum ● To liaise with the Online Safety Coordinator regularly

Role	Key Responsibilities
Network Manager/technician	● To report any online safety related issues that arise to the Online Safety Coordinator ● To ensure that users may only access the School's networks through an authorised and properly enforced password protection policy in which passwords are changed annually for pupils and every six weeks for staff during term time ● 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 ● To ensure the School's policy on web filtering is applied and updated on a regular basis ● To keep up to date with the School's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant ● To regularly monitor the use of the School network / website / remote access / email in order that any misuse or attempted misuse can be reported to the Online Safety Co-ordinator, 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 ● To keep up-to-date documentation of the School's online security and technical procedures ● To ensure that all data held on pupils is adequately protected
School Administrator	● To ensure that all data held on pupils on the School office devices have appropriate access controls in place
Teachers	● To embed online 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 ● To abide by the expected conduct (as outlined in Section 4) and participate in the education of pupils on online safety

Role	Key Responsibilities
	matters (as outlined in Section 3) when relevant to their curricular areas ● To ensure that pupils are fully aware of legal issues relating to electronic content such as copyright laws
All staff	● To read, understand and help promote the School's Online Safety Policy and guidance ● To read, understand, sign and adhere to the School's staff Acceptable Use Agreement as stated in the Information and Security Policy ● To be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current School Policies with regard to these devices ● To report any suspected misuse or problem to the Online Safety Coordinator ● To maintain an awareness of current online safety issues and guidance (e.g. through CPD) ● To model safe, responsible and professional behaviours in their own use of technology ● To ensure that any digital communications with pupils should be on a professional level and only through School-based systems, never through personal mechanisms (e.g. email, text, mobile phones, etc.) ● To ensure that the use of internet-derived materials comply with copyright law ● To ensure that pupils have no access to mobile phones at school and that mobile phones are handed into the School Administrator on arrival at school
Pupils	● To read, understand, sign and adhere to the Acceptable Use Agreement (AUA) which is sent to all pupils, annually, in September. This includes sections on general use of devices, behaviour online, emailing and use of Google Suite and Artificial Intelligence. ● To engage in online safety instruction and education as outlined in Section 3. ● To abide by expected conduct, as outlined in Section 4 as well as their annual Acceptable Use Agreement

Role	Key Responsibilities
Parents	● To read and understand the School's Pupil Acceptable Use Agreement, which is sent home at the beginning of each new academic year ● To support the School in promoting online safety and endorse the Pupil Acceptable Use Agreement which includes use of the internet and the School's use of photographic and video images ● To access the school website and app in accordance with the relevant school Acceptable Use Agreement. ● To consult with the School if they have any concerns about their children's use of technology
External groups	● External individuals / organisations will sign an Acceptable Use Agreement prior to using any equipment or the internet within the School unsupervised

Communication

This Policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the School website and saved on Teacherlink
- Policy to be part of School induction pack for new staff
- Acceptable Use Agreement discussed with pupils at the start of each year in Computing lessons
- Acceptable Use Agreement to be issued to whole school community, usually on entry to the School
- Signed Staff Acceptable Use Agreements to be held in personnel files
- Signed Pupil Acceptable Use Agreements to be held by Online Safety Coordinator

Concerns about cyberbullying and child protection

- The School will take all reasonable precautions to ensure online 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. Actions include:
    - Discussion with the counsellor/Phase Lead/Online Safety Coordinator/Head as appropriate
    - Issuing of a sanction or debit, as per the Positive Behaviour Policy
    - Informing parents
    - Removal of internet or computer access for a period
    - Referral to Police where there is potential criminal activity
- The Online Safety Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Head.
- Complaints of cyberbullying, both in and out of school, are dealt with in accordance with the Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the Safeguarding (Child Protection) Policy.

3. Education and Curriculum

Pupil online safety curriculum

In accordance with KCSIE, online safety is considered within curriculum planning. The School ensures pupils are taught how to keep themselves and others safe, including online. Pupils are educated in an age-appropriate manner about the importance of safe and responsible use of technology.

The School recognises that effective education needs to be tailored to the specific needs and vulnerabilities of individual pupils, including those who are victims of abuse, and those with special educational needs and disabilities. This is taken into account when devising and implementing processes and procedures to ensure the online safety of its pupils.

Key components of the online safety curriculum:

- To have a clear, progressive online safety education programme as part of the Computing curriculum/Wellbeing (PSHE & RSE) curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To STOP and THINK before they CLICK
- To provide online safety education in the EYFS using age-appropriate resources.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy. Pupils should understand the existence of misinformation, disinformation, and conspiracy theories online and develop critical thinking skills to evaluate sources.
- To be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be. This includes understanding how online content can present unrealistic portrayals of relationships and bodies affecting expectations and behaviour in real-life relationships.

- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private. Pupils should understand the connection between online and real-world relationship skills, including respect, consent and kindness.
- To understand the risks associated with using technology, including Artificial Intelligence, and how to protect themselves and their peers from potential risks.
- To understand the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, 'banter'.
- To understand how to respond to harmful online challenges or hoaxes.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention. This includes recognition of deepfakes and AI-manipulated content, and understanding how these technologies can be misused.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings. This includes understanding the risks of AI chatbots and the importance of not sharing personal information or relying on such bots for advice about relationships, mental health or safety.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music or video files - without permission.
- To have strategies for dealing with receipt of inappropriate materials, as well as recognising and reporting online sexual harassment (e.g. unwanted attention, comments, or image sharing).
- For older pupils: To understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, carer, teacher or trusted staff member, or an organisation such as Childline or CEOP (Child Exploitation and Online Protection Command).
- To encourage pupils who use the internet and social media to be aware of the online risks associated with extremism, radicalisation and terrorism and therefore adjust their behaviours

in order to reduce risks and build resilience (see Safeguarding (Child Protection) Policy for details).

- To ensure that internet use is age-appropriate and supports the learning objectives for specific curriculum areas.
- To ensure that outside speakers running workshops for pupils are aware of how to use apps and social media safely, as well as being aware of strategies on what to do if they feel uncomfortable or unsafe though digital mediums.
- To remind pupils about their responsibilities through an Acceptable Use Agreement which every pupil signs at the beginning of each academic year.
- To ensure staff will model safe and responsible behaviour in their own use of technology during lessons, for example, locking workstations when away from their computer, following correct personal mobile phone use guidelines, etc.
- To ensure that, when copying materials from the web, staff and pupils understand issues around plagiarism; to check copyright and also to know that they must respect and acknowledge copyright/intellectual property rights.
- To ensure that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups, buying on-line, on-line gaming, and gaming monetisation.
- To use Artificial Intelligence safely and productively – including the understanding of intellectual property and plagiarism, as well as implications of data privacy when using AI online.

RSE and Online Safety Integration

The School recognises that online safety education must be closely integrated with Relationships and Sex Education.

Pupils will learn:

- How online friendships and interactions should follow the same principles of kindness and respect as face-to-face relationships
- That private body parts remain private online and offline, and they should never share or be asked to share images of private body parts
- How to recognise when online communication makes them feel uncomfortable and who to tell

Staff and Governor Training

The School:

- Ensures staff are aware that technology can play a significant part in many safeguarding and wellbeing issues, and that pupils are at risk of abuse online as well as face-to-face. At times, abuse can also take place concurrently online and in a pupil's daily life and this can include child-on-child abuse.

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Makes regular training available to staff on online safety issues and the School's online safety education program. This includes support in identifying high quality resources for the teaching of technology safety, sharing of images, cyberbullying and dealing with harmful online challenges and hoaxes.
- Provides, as part of the induction process, all new staff (including those on university/college placements and work experience) with information and guidance on the Online Safety Policy and the School's Acceptable Use Agreements.
- Ensures all staff are familiar with and understand the online safety protocols for identifying and reporting concerns, including safeguarding concerns. This is delivered through new staff induction, staff meetings and Pastoral Leadership meetings.
- Ensures safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school safeguarding approach.
- Ensures all Governors are equipped with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures of the School are effective and to support the delivery of a robust whole school approach to safeguarding and child protection. This is delivered through appropriate safeguarding and child protection training, which includes online safety.

Parent Awareness and Training

The School runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of safe online behaviour are made clear;
- Information on which systems are in place to filter and monitor their child's online use. On the school network, or when logged into their pupil Google account on the Chromebook at home, this includes Senso and Smoothwall
- Clear information given alongside Home Learning on use of Google Classroom and which sites they will be asked to access
- Clear information given on online communication via Google Classroom for pupils
- Information leaflets, School newsletters, the School website and app
- Talks, presentations and practical advice sessions held at school
- Suggestions for safe internet use at home
- Provision of information about national support sites for parents

4. Expected Conduct and Incident Management

Expected conduct

In the School, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Agreement (AUA) which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Need to understand the importance of adopting good online safety practice when using digital technologies out of School and realise that the School's Online Safety and Staff Behaviour Policy covers their actions out of School, if related to their membership of the School.
- Are expected to know and understand School Policies on the use of personal mobile phones, digital cameras and hand-held devices. They must also know and understand school policies on the taking of and use of images.

Staff:

- Are responsible for reading the School's Online Safety Policy and using the school ICT systems accordingly, including the use of personal mobile phones and hand-held devices.
- Must follow the Staff Code of Conduct and Acceptable Use Agreement.
- Should be aware of emerging online risks including AI-generated content, deepfakes, and online relationships abuse, and how these may manifest in pupil behaviour or disclosures.
- Should understand the links between online safety concerns and broader safeguarding issues, and should recognise that online safety incidents carry the same gravity, which may require referral under child protection procedures.

Pupils:

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Should know and understand that filtering and monitoring software (Smoothwall and Senso) remains active any time they are logged into their School Google account – both in School and at home on their Chromebooks.

Parents:

- Should provide consent for pupils to use the internet, as well as other technologies, as part of the Acceptable Use Agreement form at the time of their child's entry to the School.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

- Should support the School's adherence to regulatory online safety requirements, including not uploading or sharing videos and/or photographs on personal mobile phones or devices, of pupils other than their own children without permission of that child's parent/s.
- Are requested to turn off or keep their phones and other devices with image taking or sharing capabilities on silent and ensure they remain out of sight of any pupils until they leave the premises.

Incident Management

In the School:

- Auto-lock system applies to all staff computers.
- Searches and web addresses are monitored and the IT technicians will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.
- There is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions; though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and the wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the School's escalation processes.

In the event of an online safety incident:

- The concern should be reported to the Online Safety Co-ordinator, who will inform the DSL and Head, as appropriate. If the incident gives rise to an online safeguarding concern, it should be referred straight to the DSL who will follow the Safeguarding (Child Protection) Policy.
- The Online Safety incident will be logged on CPOMs, using the 'Online Safety' tag and all actions will be recorded.
- Where necessary, support is actively sought from other agencies as needed (e.g. CEOP, UK Safer Internet Centre helpline, etc.) in dealing with online safety issues.
- Monitoring and reporting of online safety incidents via CPOMS takes place and contributes to developments in policy and practice in online safety within the School.
- Parents are specifically informed of online safety incidents involving young people for whom they are responsible. Support is offered to parents in how to talk to their daughter about the incident and, if appropriate, how online safety rules and filtering software can be utilised at home.
- The police will be contacted if staff or pupils receive online communication that the School considers particularly disturbing or breaks the law.
- Pupils are able to report any online safety concerns through the Online Worry box, which can be found through a link on Google Classroom.
- Should an incident involve a staff member, this would be passed to the Head who would refer to the staff code of conduct and/or Acceptable Use Agreement.

Types of incidents requiring immediate DSL referral:

- Any incident involving AI-generated sexual imagery
- Online sexual harassment between pupils
- Incidents involving conspiracy theories or extremist content that may indicate radicalisation risks
- Gaming or gambling-related concerns that suggest addiction or financial harm

5. Managing the ICT Infrastructure

Passwords - see Information Security Policy for details

E-mail - see Information Security Policy for details

School website – see Information Security Policy for details

Social networking - see Information Security Policy for details

Video Conferencing - see Information Security Policy for details

CCTV - see Information Security Policy for details

6. Equipment and Digital Content and Use

Personal mobile phones and mobile devices

- Personal mobile phones and other electronic devices with image taking or sharing capabilities are brought into School entirely at the staff members', pupils' & parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into School.
- Staff members may use their personal mobile phones during school break times but never in the presence of pupils and preferably in the Staff Room. All visitors are requested to turn off or keep their phones on silent and ensure they remain out of sight of any pupils until they leave the premises. In line with the Safeguarding (Child Protection) Policy, all devices with image taking or sharing capabilities (including mobile phones, smart watches, etc.) must be turned off and stored in EYFS.
- The recording, taking and sharing of images, video and audio on any personal mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head. All mobile phone use is to be open to scrutiny and the Head is able to withdraw or restrict authorisation for use at any time if it is deemed necessary.
- 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.

- Where parents or pupils need to contact each other during the school day, they should do so only through the School office's telephone. If a staff member is expecting a personal call, they may leave their phone with the School office to answer on their behalf, or seek specific permission to use their phone other than their break times.

Pupils' use of personal devices

- When pupils sign the Acceptable Use Agreement, it is recommended to parents that they set ground rules for use of personal devices in a similar manner to the AUA.
- The School acknowledges that outside of the School setting, when not using school devices with filtering and monitoring software, pupils may have unlimited and unrestricted access to the internet and mobile phone networks. The School encourages parents to monitor technology use and check that filtering systems are in place.
- The School strongly advises that pupil mobile phones should not be brought into school. Only Year 6 pupils who are making their own way to and from school are permitted to bring a phone to School. When in School, these pupils are required to turn off and hand in their mobile phone to the School office and collect it at the end of the day. Pupils should not wear smart watches which have internet or mobile network access.
- If a pupil breaches this Policy, then the phone or device will be confiscated and will be held in a secure place in the school office and parents will be informed. The Positive Behaviour Policy would be followed to address this breach.
- If a pupil needs to contact her parents or carers, they will be allowed to use a school phone. Parents should not contact their child via their mobile phone during the school day but instead contact the school office.
- Pupils are given advice about how to protect their phone numbers, by only giving them to trusted friends and family members. Pupils will be given guidance and advice about safe and appropriate use of mobile phones and personally owned devices, and will be made aware of boundaries and consequences e.g. not sharing login details for apps or social media.
- Pupils must turn off cellular data if bringing a device into School, e.g. a kindle.
- Cyber-bullying by pupils via texts and emails will be treated as seriously as any other type of bullying and will be managed through the School's anti-bullying procedures.

Staff use of personal devices

- Staff are not permitted to use their personal mobile phone numbers for contacting children, young people or their families within or outside of the setting in a professional capacity, unless given explicit permission from the Head to contact caregivers in circumstances such as residential trips.
- Staff will be issued with a School phone where contact with pupils, parents or carers is required. In an emergency where a staff member does not have access to a School-owned device, they should use their own device and hide (by inputting 141) their own mobile number for privacy purposes.

- Mobile phones and personally owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off, and mobile phones or personally owned devices must not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances. Staff may be required to use their personal devices to access CPOMS, however this should also be done outside of lesson time and not in the presence of pupils. In line with the Safeguarding (Child Protection) Policy, in EYFS all devices with image taking or sharing capabilities (including mobile phones, smart watches, etc) must be turned off and stored.
- 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 a member of staff breaches the School's policy on personal device use, disciplinary action may be taken.

Social Media

Social media is an increasingly influential part of life particularly for young people. 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 young people from extremist narratives and *Prevent* can play an active part in this process.

In this School:

- Social networking sites and unfiltered AI-chatbots will be blocked using a suitable filtering system (Smoothwall) 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, pupils or visitors find unblocked harmful content, including extremist content, AI-generated sexual imagery or serious misinformation, they must report it to the Designated Safeguarding Lead and the Online Safety Co-ordinator/DDSL, or in their absence, a senior member of staff.

The Prevent Duty (see also Safeguarding (Child Protection) Policy)

- The School ensures that pupils 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 pupils 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 school's Computing curriculum and is also embedded in Wellbeing (PSHE & RSE).
- 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 Agreement (AUA) for staff and visitors, or Acceptable Use Agreement (AUA) for pupils and parents, refers to preventing radicalisation and related extremist content.
- Staff are required to report any online terrorist related material visit: www.gov.uk/report-terrorism (see Safeguarding (Child Protection) Policy for more details)

Digital Images and Video

- Under the Data Protection Act 1988, at the start of each academic year, parental consent to the taking and use of photographs and videos will be updated for each pupil.
    - Consent for External Media in Public Areas: Photographic images and videos of pupils will appear on the public area of the School's website, marketing literature, social media channels, and carefully selected organisations with granted consent for External Media in Public Areas. Names will never be identifiable on images and videos published.
    - Consent for Media in Private Areas: Photographic images and videos of pupils will appear on the password-protected Parent Area of the School's website, display and boards within the School, weekly newsletters (Bute Insights) and annual yearbook (Bute Tribute). Names will never be identifiable on images and videos published.
- Social Media Accounts: the School has LinkedIn and Instagram feeds accessible by the general public.

Use of Images

- No images of pupils, staff or parents should be published onto the School's social media feeds and public area of the website without the written consent of parents/carers. The agreement to consent to use of images on social media is included in the consent form signed annually and recorded on SIMS. Staff must not identify by name pupils featured in photographs, or allow personally identifying information to be published on School social media accounts or public area of the School's website.
- All names will be blurred completely or cropped if possible.
- Pupils who do not have consent for Media in Public Areas and/or Media in Private Areas will be asked not to participate in photography for these areas, where possible. If they are visible, they will be cropped out of the photo or their face will be masked by either blurring or a covering image.
- Care will be taken to ensure that pupils' images are used appropriately. If the pupils appear in anything other than their full school uniform, e.g. swimming costumes, the photo will be cropped appropriately.
- Regarding the use of hashtags within the School's social media platforms (currently LinkedIn and Instagram): as far as possible hashtags should be used which are relevant to the post specifically, however, a mixture of local and generic hashtags is acceptable. Hashtags should be kept to a minimum of one to two per post to make a relevant connection to the post.

Hashtags should be researched to discover their appropriateness to extend the reach of the post and to ensure, as far as possible, that the hashtag does not link to inappropriate posts / tweets.

- Staff sign the School's Acceptable Use Agreement (AUA) and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- Only School cameras or School mobile phones can be used to take photographs of pupils.
- Photographs are stored on computers which are password protected.
- In their online safety education programme, pupils are taught about how images can be manipulated and are also taught to consider how to publish for a wide range of audiences which might include Governors, parents or younger children as part of their Computing scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make personal information, public. Pupils are also given instruction through the Computing curriculum related to age-restrictions on social media websites and the rationale behind these restrictions.
- Pupils are taught that they should not post images or videos of others without their permission. The School teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The School teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- 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 school (e.g. theatre groups or workshop providers) are not to photograph or film pupils without parents' permission.

Record Keeping

The School manages all records created in line with this Policy in accordance with the Information Security Policy. All serious incidents concerning online safety are logged on CPOMs. The School recognises these records often contain personal data. The use of any personal data is in accordance with the data protection law and the Information Security Policy.

Asset Disposal - see Information Security Policy for details

Details of all School-owned hardware will be recorded in a hardware inventory.

Details of all School-owned software will be recorded in a software inventory.

All redundant equipment that may have held personal data will have the storage media forensically wiped if sending to third party companies. Alternatively, if the storage media has failed, it will be physically destroyed. The School will only use authorised companies who will supply a written guarantee that this will happen.

7. Monitoring and Review

The Online Safety Policy is referenced in other School Policies: ICT and Computing Policy, Safeguarding (Child Protection) Policy, Anti-Bullying Policy, Information and Security Policy and in the School Development Plan, Positive Behaviour Policy, Wellbeing Policy, and Relationships and Sex Education and Health Education (RSHE) Policy.

- The Governing Body has overall responsibility for this Policy and is responsible for working with the DSL and Online Safety Coordinator on document ownership, review and updates.
- The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the School.
- The Online Safety Policy has been written by the School's Online Safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the Policy and it has been agreed by the SLT and approved by Governors. All amendments to the School Online Safety Policy will be discussed in detail with all members of teaching staff.