Online Safety policy
(incorporating mobile phone and camera policy)

St Christopher's Preparatory School

September 2025

Member of staff responsible: Head/Deputy/ICT Coordinator

Last reviewed: September 2025

Policy witnessed and signed by School Proprietor & Chair of Governors:

Mr A Mehta

Mr D Tidmarsh

Contents

STATUTORY REQUIREMENTS

The Inspired Learning Group's Independent Schools have a statutory requirement under Sections 27 and 47 of the Children Act 1989 to assist the Local Authority Social Services Department acting on behalf of children in need or enquiring into allegations of child abuse. The Schools will safeguard and promote the welfare of children in compliance with DfE guidance *Keeping Children Safe in Education (2025) (KCSIE)* and associated guidance *Working Together to Safeguard Children (2013) (WTSC)*. We also comply with the "Statutory guidance on children who run away or go missing from home or care (2014)".

1. Introduction and Overview

St Christopher's Preparatory School is committed to ensuring that our children are able to use existing and emerging technologies safely. We recognise that the internet and other digital technologies provide a vast opportunity for children to learn. These technologies allow those working / volunteering with children to promote creativity, stimulate awareness and enhance learning. With the desire for children/young people to access every opportunity for learning, there is also the need to keep them safe from the risks of the internet and digital and mobile technologies. St Christopher's School is committed to ensuring that those who work/volunteer with children/young people are aware of the dangers that exist so they can take an active part in safeguarding children/young people.

Scope

This policy should be regarded as work in progress and will be amended following national / regional advice and as the school's network and peripherals are developed.

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at St Christopher's with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of St Christopher's
- assist school staff working with children 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/or 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 our 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), 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
- being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism,

radicalisation, extremism, misinformation, disinformation (including fake news), conspiracy theories, deepfakes, and other AI-generated content that may mislead or harm.

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords
- being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

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) (Ref Ofsted 2013)
- 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

Commerce

- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams

We will ensure our online safety policies and practices recognise these as safeguarding issues. Our Filtering/monitoring systems will be audited termly to see whether they catch or flag problematic false/misleading content.
Training of staff will include how to identify and respond to these kinds of harms.

Scope

This policy applies to all members of St Christopher's community (including staff, pupils / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / school ICT systems, both in and out of St Christopher's.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Role	Key Responsibilities
Headteacher / Deputy Headteacher	• take overall responsibility for online safety provision • take overall responsibility for data and data security • ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. ILG • be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • be aware of procedures to be followed in the event of a serious online safety incident • receive regular monitoring reports from the Online Safety Co-ordinator / Officer • ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager)

IT Specialist	• takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies /documents
	• promotes an awareness and commitment to e-safeguarding throughout the school community
	• ensures that online safety education is embedded across the curriculum
	• liaises with school/ILG ICT technical staff
	• communicates regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering / change control logs alongside the DSL.
	• ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
	• ensure that an online safety incident log is kept up to date or that online safety incidents are logged in other school logs (behaviour-bullying) to avoid proliferation of information databases
	• facilitates training and advice for all staff
	• regularly updated in online 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

ILG Directors / Online safety delegate – Technology Firm RIKA	• ensure that the school follows all current online safety advice to keep the children and staff safe • approve the Online safety Policy and review the effectiveness of the policy. This will be carried out by the Directors receiving regular information about online safety incidents and monitoring reports. • support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the Directors will include: • regular review with the Online safety Co-ordinator including online safety incident logs, filtering / change control logs) • review compliance with DfE Filtering and Monitoring Standards and self-assessment outcomes as part of safeguarding oversight.

Role	Key Responsibilities
Computing Curriculum Leader	• oversee the delivery of the online safety element of the Computing curriculum • liaise with the online safety coordinator regularly
RIKA Network Manager/ technician	• report any online safety related issues that arises, to the online safety coordinator. • ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • ensure that provision exists for misuse detection and malicious attack 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 • the school's policy on web-filtering is applied and updated on a regular basis • ILG & DSL is informed of issues relating to the filtering applied • that he / she keeps 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 • that the use of the *network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Online safety Co-ordinator / Officer /Headteacher for investigation / action / sanction* • 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 e-security and technical procedures
Curriculum Director	• To ensure that all data held on pupils on Data Management Programme is adequately protected
RIKA Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
ILG Nominated contact(s) RIKA	• To ensure all ILG services are managed on behalf of the school including maintaining the ILG database of access accounts
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 and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and 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 policies and guidance • To read, understand and adhere to the school Online Safety Policy • To be aware of online safety issues related to the use of mobile phones, cameras and handheld 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

Role	Key Responsibilities
	• 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.
Pupils	• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and handheld devices. • to know and understand school policy on the taking / use of images and on cyber-bullying. • 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 Policy covers their actions out of school, if related to their membership of the school • to take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of online safety policies
Parent Liaison	• Educating Parents and raising awareness as instructed by Head in newsletters, parents evening and parent Awareness Training
Parents/carers	• to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement and the school's use of photographic and video images • to access the school website / Data Management Programme / on-line pupil / pupil records 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	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication:

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

- Policy to be posted on the school website and office folder/ internal teacher share drive/ Computer Room
- Policy to be part of school induction pack for new staff
- Acceptable use agreements to be issued to whole school community, usually on entry to the school

Handling complaints:

- 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. Neither the school nor the Local Authority can 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:
  - interview/counselling by teacher / Headteacher / Online safety Coordinator
  - informing parents or carers;
  - removal of Internet or computer access for a period
  - referral to ILG/ LA / Police.

- Our Online safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The online safety policy is referenced from within other school policies: ICT and Computing policy, Safeguarding policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The online safety policy will be reviewed annually or when significant new technologies, emerging risks, or updates in statutory guidance arise.
- The online safety policy has been written by the school 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 Directors and other stakeholders such as the PTA. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil online safety curriculum

This school

- Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on e-safeguarding and e-literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
  - to STOP and THINK before they CLICK
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know how to narrow down or refine a search;
  - [for older pupils] 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;
  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - to understand why on-line '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;
  - 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 files - without permission;
  - to have strategies for dealing with receipt of inappropriate materials;
  - [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 or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures 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 / gambling
- Ensures pupils will be educated on emerging online risks including AI misuse, deepfakes, misinformation, and anonymous platforms.

Social Media Safety

The School's Social Media Safety policies continue to be in place.

- all children have signed the school's School Internet Usage Rules to underpin their awareness of online safety
- the School's 'Cameras, Video and Social Media Acceptable Use By Parent and Pupils Policy' is signed by all parents
- it has been reinforced that staff must only contact pupils through a registered School online programme such as Zoom and Showbie, with the recommendation that security ID and Passwords are changed regularly
- pupils, parents and staff have had expectations and safety rules made clear in written communication

One-to-one online meetings between Pupils and Staff

There may be a need for a member of staff to have a one-to-one meeting with a pupil. If this is the case the following two rules must be adhered to;

- a record should be kept of such meetings and a senior member of staff should be informed the meeting is happening, ideally the Headteacher

- a responsible adult should be with the pupil at all times during the meeting

Staff and Director training

This school

- 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; annual updates/ termly staff meetings etc.
- Staff training will be updated annually or when necessary, to reflect new and emerging online risks (e.g. misinformation, AI misuse, deepfakes, scams)."
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This 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 e-safe behaviour are made clear
  - Information leaflets; in school newsletters; on the school web site;
  - demonstrations, practical sessions held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (KS1: it would be expected that parents/carers would sign on behalf of the pupils.)
- 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
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school
- all forms of online harassment and peer-on-peer abuse will be taken seriously. Behaviour dismissed as 'just banter' will not be tolerated where it causes harm.
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form at 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

Incident Management

In this school:

- 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 its 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.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school's senior leaders and Directors.
- parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school:

In accordance with the DfE Filtering and Monitoring Standards (2023). We will use the 'Test Filtering' system for regular self-assessment. - Governing bodies and proprietors should review the standards and discuss with SLT and IT staff and service providers if improvements need to be made

- Has the educational filtered secure broadband connectivity
- Uses a secure filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to Rica who hold the approved 'web filtering management' status;
- Ensures network healthy through use of regularly updated anti-virus software and network set-up so staff and pupils cannot download executable files;
- Uses secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons (Within IT);
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;

- Works in partnership with the ILG to ensure any concerns about the system are communicated so that systems remain robust and protect pupils;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's First Steps data management system as a key way to direct pupils to age / subject appropriate web sites;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Swiggle, Kiddle or Google Safe Search.
- Is vigilant if and when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Teacher's to use Apple Classroom to view and monitor each pupil's iPad activity in lessons.
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the teacher. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or ILG Helpdesk as necessary;
- 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;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – the ILG Directors, Police – and the LA.

Network management (user access, backup)

This school

- Has log-ins for all their devices and pupils where necessary;;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Ensures the Systems Administrator / network manager is up-to-date with ILG and school policies /
- Storage of all data within the school will conform to the UK data protection requirements
  Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- The school's management information system is stored using a cloud-based system, using Microsoft One Drive.
- Staff access the schools' management information system on One Drive with their own username and password.
- Staff can access one drive from their Laptop and iPad.
- Staff will save work either to One Drive or to their Apple iCloud.
- Staff and pupils do not share any devices.
- Pupils work on their own individual iPads, where they cannot access anyone else's data or files.
- All pupil's work is saved to their own individual Apple iCloud account, which can be retrieved in the event of an iPad being lost or broken.

- The iPad can be put into lost mode and locked in the event of an iPad going missing or broken.
- Has set-up the network so that users cannot download executable files / programmes
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with ILG policies, practices/procedures *e.g. Email or Intranet; finance system, Personnel system etc.*
- Maintains equipment to ensure Health and Safety is followed;
  e.g. all electrical equipment is checked by approved suppliers/LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module

- Ensures that access to the school's network resources from remote locations by staff is restricted to approved systems;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. parents using a secure portal to access information on their child;
- Provides pupils and staff with access to content and resources through the approved Data Management Programme which staff access using their username and password ;
- Makes clear responsibilities for the daily back-up systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Generative AI: Product Safety Expectations - any AI tools being used or we are considering using, must satisfy safety expectations. Filtering, moderation, data protection will be checked. Should we consider using AI in classrooms all staff will be trained on how to integrate AI safely and understand risks.
- Filtering and Monitoring – we will use the *'Plan technology for your school'* (test filtering) to assess our current systems and identify areas for improvement. This will aim to be proactive with cybersecurity risks (e.g. regular reviews, updates).
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our system.

E-mail

This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
  - Does not publish personal e-mail addresses of staff on the school website. We use anonymous, class teacher names or group e-mail addresses, for example admin@schoolname.org.uk head@schoolname.org.uk / or class teacher e-mail addresses for communication with the wider public.
  - Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
  - Will ensure that email accounts are maintained and up to date
  - Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
  - Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language

Pupils:

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
  - that an e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments;
  - embedding adverts is not allowed;
  - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages;
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;

- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with (if applicable).

Staff:

- Staff only use e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;

- All staff sign our school Agreement Form AUP to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to authorised staff
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. admin@stchristophersschool.org.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached, and permission must be given by parents
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Learning platform

- Uploading of information on the schools' share and academic drives is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools share drive will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, to a designated pupil area

Social networking

- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, nor to befriend or comment on pupils social pages – in other words to avoid any such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
-

Video Conferencing/Zoom/Teams/MT

This school

- Does not video conference currently. If and when this is introduced then only approved with approved sites and on checked webcam sites;
- School uses Zoom/Teams calls for remote learning/meetings when needed

CCTV

- CCTV is part of our site surveillance for staff and pupil safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- Staff are clear who are the key contact(s) for key school information.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in the Single Central Register.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - staff,
  - Directors,
  - pupils
  - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.

- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.

Technical Solutions

- We require staff to log-out of systems when leaving their computer
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We use cloud-based storage
- No portable equipment is permitted to be loaned by the school in general. However, during lockdown situations staff/pupils have access to borrowed ipads/laptops for teaching/learning.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

Responsibility

- Mobile phones and personally-owned mobile devices brought into school are entirely at the staff member or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school
- 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 handheld 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 to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- Mobile phones and personally-owned devices approved for use by the Head in exceptional circumstances are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

Staff

- All staff (EYFS and School) mobile phones must be secured in the locked cabinets/drawers provided
- Staff members may use their phones during school break times in certain areas.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be directed towards the use of the school phone when contact with pupils, parents or carers is required. Staff will be permitted to use their own mobile phone whilst on educational off-site visits, in case of emergencies only

- Approved by Head 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 will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- 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 – e.g. school teacher iPads
- If a member of staff breaches the school 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, they may use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Visitors

All visitors are requested to keep their phones on silent.

Parents and Pupils

- Where parents or pupils need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. 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 permissions to use their phone at other than their break times.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- 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.

Pupils' use of personal devices

- Pupil mobile phones should not be brought into school.
- 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 (Year 6/summer term if allowed to walk travel home alone)
- 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. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into tests of examinations in or out of St Christopher's. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone.
- No pupils should bring his or her mobile phone or personally owned device into school. Any device brought into school will be confiscated.

Digital images and video

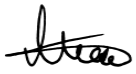
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced videos.
- Staff comply with the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include Directors, parents or younger children as part of their ICT 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 public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- 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 will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. 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

Signed by Proprietor



Mr A Mehta