



Digital Safety Policy – Section One

Document Reference	ICT-POL-004-S001
Version/Revision	v4.0
Effective Date	May 2025
Review Date	May 2027
Author(s)	Director of IT, ELT
Reviewer(s)	ELT
Applicable to	Whole School

Revision History

Version	Date	Reason for most Recent Revision
v1.0	October 2016	New Policy
v1.1	November 2017	Minor changes
v2.0	March 2019	Minor changes
v3.0	March 2022	Renamed Digital Safety Policy. Other changes made
V4.0	May 2025	Additional sections added: Third-Party Applications, VPN Use & AI. Edits to Key Responsibilities



Contents

1 INTRODUCTION AND OVERVIEW	2
1.1 PURPOSE	2
1.2 Communication	4
1.3 Handling Incidents	4
1.4 MAIN AREAS OF RISK	4
Content	4
Contact	4
Conduct	4
2 EDUCATION AND CURRICULUM	4
2.1 Pupil Online Safety Curriculum	4
2.2 Staff Training	5
2.3 Parent Awareness and Training	5
3 EXPECTED CONDUCT AND INCIDENT MANAGEMENT	5
3.1 All Users	5
3.2 Staff, including Temporary (“Supply”) Staff	5
3.3 Parents/Carers	5
3.4 Incident Management	5
4 Managing IT and Communication Systems	6
4.1 Internet Access, Security (Virus Protection) and Filtering	6
4.2 Network Management (User Access, Backup)	6
4.3 Password Policy	7
4.4 Email	7
4.5 Social Networking	7
5 Data Security: Management Information System Access	8
6 Data Security: Google Suite for Education	8
7 Use of Third-Party Applications and Data Sharing	8
8 Prohibited Use of VPNs on the School Network	8
9 AI - Artificial Intelligence	9
10 Equipment and Digital Content	9
10.1 Mobile Devices (mobile phones, tablets and other mobile devices)	9
10.2 Pupils’ Use of Personal Devices	10
10.3 Staff Use of Personal Devices (owned by the School or by the Staff Member)	10
10.4 Digital Images and Video	11
11 Key Responsibilities	11
11.1 Principal	11
11.2 Heads of School	11
11.3 Director of IT	11
11.4 Head of Digital Learning	12
11.5 Members of the Board of Governors	12



DIGITAL SAFETY POLICY - SECTION 1

ICT-POL-004-S001 |v3.0|Effective Mar 2022

11.6 Computing Curriculum Subject Leaders	12
11.7 Teachers	12
11.8 Staff	12
11.9 Pupils	12



1 Introduction and Overview

1.1 Purpose

This policy sets out the key principles regarding safe digital practices and the structures and expectations that will support the policy.

And should be read in conjunction with the following:

- Mobile Device Acceptable Use – Pupil [ICT-POL-004-S002]
- ICT Acceptable Use – Pupil [ICT-POL-004-S003]
- ICT Acceptable Use – Staff [ICT-POL-004-S004]
- Safeguarding Children & Safer Working Practice Policy – [HRF-POL-011]
- Artificial Intelligence Use Policy

Privacy Policy

St Christopher's School will:

- Safeguard and protect children and staff when engaged in digital activities.
- Set clear expectations of behaviour relevant to responsible use of the internet for educational, personal or recreational use for pupils, staff and others who access school digital resources.
- Ensure that clear methods are in place to deal with the misuse of the School's digital facilities.
- Ensure that the educational programme includes all aspects of safe internet use and what pupils should do if faced with digital abuse, manipulation or coercion.
- 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 erroneous or malicious allegations against adults who work with pupils.

1.2 Communication

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

- The policy and AUPs are posted on the School's website and are included in staff handbooks. Updates will be posted as necessary.
- The policy is part of the school induction pack for new staff and will be specifically addressed during induction processes.
- Relevant AUPs are made available to all users via the St Chris Cloud, St Chris Connect, and School Website.
- Computing departments will refer to the pupil AUPs within the curriculum lessons. Older students joining at KS4 and KS5 will be provided with this information during induction.

1.3 Handling Incidents

- The School will take all reasonable precautions to ensure digital safety.
- Staff and pupils are aware of how breaches will be handled.
- Incidents and breaches will be reported on the same day they are discovered to the relevant line manager .
- Concerns about staff misuse will be referred to the Head of School or Principal, as appropriate. A concern about the Head of School will be referred to the Principal. A concern about the Principal will be referred to the Chairperson of the Board of Governors.



1.4 Main Areas of Risk

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

Content

- Violent, racist, sexually explicit content.
- Websites promoting harmful behaviours.
- Hate or derogatory content.
- Doubtful authenticity and accuracy of online content (fake news, etc).

Contact

- Grooming (sexual exploitation, or sexual manipulation, etc).
- Bullying using technology in all forms.
- Social or identity theft, including impersonation or obtaining passwords.

Conduct

- Aggressive, coercive, manipulative, unpleasant and other inappropriate behaviours.
- Privacy issues, including disclosure of personal information.
- Creation of a harmful or damaging digital footprint and online reputation.
- Excessive amount of time spent on devices (passive watching, etc)..
- Gambling, sexting, accessing inappropriate or dangerous websites, including social media.
- Disregard for the privacy of others, intellectual property and ownership, whether copyrighted or not.

2 Education and Curriculum

2.1 Pupil Online Safety Curriculum

The School:

- Has a whole-school Digital Leadership Framework and a clear online safety education programme covering skills, attitudes and behaviours appropriate to pupils' age and experience.
- Ensures that digital activity is age-appropriate, as supported by FRC learning objectives within specific curriculum areas.
- Reinforces pupils' knowledge of their responsibilities through the pupil AUPs.
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of digital technology.
- Ensures that staff and pupils understand issues around plagiarism and academic dishonesty; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.

2.2 Staff Training

The School:

- Ensures that staff are formally trained at least every two years with regard to online safety issues and, in addition, whenever needed to cover new issues, regulations or legislation.
- Provides as part of the new staff induction process, information and guidance on the Digital Safety Policy and the School's AUPs.

2.3 Parent Awareness and Training

The School:



- Provides induction materials for parents, which include online safety.
- Offers online safety advice and guidance for parents.

3 Expected Conduct and Incident Management

3.1 All Users

- Are responsible for using the school IT and digital systems in accordance with the relevant AUPs and are made aware of the consequences of breaches.
- Must report abuse, misuse or access to inappropriate materials and understand how to do so.
- Will adopt good digital safety practice when using technologies within the school community.
- Know school policies on the use of mobile devices including cameras.

3.2 Staff, including Temporary (“Supply”) Staff

- Will be vigilant at all times, as far as is reasonable and with regard to the age of pupil, when working with pupils engaged in digital activities.
- Take all reasonable precautions when working with pupils using the internet for research.

3.3 Parents/Carers

- Are made aware of the School’s rules for appropriate use and what sanctions result from any misuse.
- Will report any concerns to the School through appropriate channels.

3.4 Incident Management

- The Digital Safety Policy is strictly applied and is monitored for compliance.
- Breaches of this policy by pupils are dealt with through age-appropriate sanctions.
- Breaches by staff are treated as disciplinary matters.
- Breaches by other users are dealt with on an ad-hoc basis as agreed by the Principal.
- All members of the school community are encouraged to be conscientious in reporting issues.
- Digital incident logs are examined and contribute to developments in policy and practice.
- Parents/carers are informed of online safety incidents involving pupils for whom they are responsible.
- The School may refer any suspected illegal material to the appropriate authorities.

4 Managing IT and Communication Systems

4.1 Internet Access, Security (Virus Protection) and Filtering

The School:

- Informs all users that Internet and email activity is monitored.
- Has appropriately filtered secure broadband connectivity, which blocks, as far as is reasonably possible, inappropriate sites.
- Has effective anti-virus software installed.

4.2 Network Management (User Access, Backup)

The School:

- Uses individual, audited log-ins for all users.
- Has cloud activity monitoring/auditing software installed.
- Takes incremental daily back-up of school data stored in Google Drive (administrative and curriculum).



To ensure the network is used safely, the School:

- Provides pupils with a unique username and password to access the Internet and other services.
- Ensures that no one is permitted to log in as another user.
- Provides staff with Internet, email access and cloud access through a unique, audited username and password.
- Uses permissions to secure documents and Shared Drives so that only authorised users can view/edit/distribute documents.
- Requires users to log off when they finish working or are leaving the computer unattended.
- Ensures that school devices have adequate virus protection.
- Makes clear to staff that they are responsible for ensuring that any device loaned to them by the School, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure electrical and mechanical safety.
- Ensures that access to the School's cloud resources from remote locations is audited and secure.
- Does not allow outside agencies to access our network remotely, except where there is a clear, professional need, in which cases access is audited and restricted and is only through approved systems.
- Transfers data securely.
- Has wireless networks that are secured to industry standards and are suitable for educational use.

4.3 Password Policy

- Staff and pupils are required to keep their passwords private and if a password is compromised, are required to notify school immediately.
- Staff and pupils are advised to use strong passwords.

4.4 Email

The School:

- Provides staff with an individual email account for professional use. Limited personal use is accepted, provided the nature of the content does not contravene the Digital Safety Policy.
- Provides pupils with an individual email account for school use.
- Teaches pupils the appropriate use of tone, language and content of emails.
- Will take appropriate action if any member of staff or pupil receives an email that is considered to be disturbing or breaks the law.

4.5 Social Networking

Staff:

- Will keep professional and private accounts separate.
- Teachers will not use their personal social media sites for school purposes and will not have pupils as "friends" on any such site.
- Teachers must not accept invitations from pupils to be "friends" on social media sites /accounts.
- Teachers will apply appropriate privacy settings to any social media or other digital communications medium in order to protect themselves and pupils and to restrict membership to appropriate pupils only.
- Teachers will adhere to the minimum age restrictions that the School sets for specific social media sites.

Members of Staff in Private Use will:

- Not be online "friends" with any pupil.



- Not engage in online discussion with third parties on personal matters relating to members of the school community.
- Will not attribute their personal opinions to the School.
- Ensure that their personal opinions and/or the content of their online presence in social media and other entities, do not compromise their professional standing.
- Ensure their digital behaviour does not bring, or risk bringing the School into disrepute.
- Regularly check security settings on personal social media profiles so as to minimise risk of accidental privacy/sharing.

Pupils:

- Are taught about social networking, acceptable behaviours, age restrictions and how to report misuse, intimidation or abuse.
- May only use social media in lessons where specifically authorised by a member of staff for a specific educational purpose.
- Must not invite members of staff to be online “friends”
- Must, in their use of social media inside or outside of school, exhibit appropriate behaviour. Behaviour that harms or seeks to harm other pupils, including bullying, harassment, coercion or manipulative behaviour and sending inappropriate material to a pupil, will be reported to parents and, possibly, appropriate authorities. In certain cases of inappropriate behaviour outside of school, the School also reserves the right to take disciplinary or other action.
- Use of social media and other means of communication used outside of school, must not damage the reputation of the School or any employee or pupil of the School.

Parents:

- Will be provided with information regarding digital safety through home/school communications and curriculum information.

5 Data Security: Management Information System (MIS) Access & Google Workspace for Education (GWE)

- All data is encrypted and stored securely off-premise in the cloud.
- Staff are required to log-out or lock systems when leaving their computer.
- Two-factor authentication (2FA) is used to add an extra layer of security to our MIS (which stores personal and sensitive data) and to the GWE applications and documents(which stores personal and sensitive data).

6 Google Workspace for Education

The School’s core learning management system (LMS) is Google Workspace for Education (GWE), a suite of secure, cloud-based tools designed to support teaching and learning. GWE enables the School to provide a secure learning environment, enhance instructional impact, and prepare students with the digital skills needed for the future.

GWE core tools include Gmail, Calendar, Docs, and Classroom. Depending on their year group, students may also have access to additional Google services, including, but not limited to:

- Educational and Creative Tools: Applied Digital Skills, Colab, CS First, Search and Assistant, Chrome Canvas, Cursive
- Web and Productivity Tools: Web Store, Alerts, Bookmarks, Books, Groups, Translate



- Maps: Earth, Maps, My Maps
- Media and Backup: Photos, Play, YouTube, and third-party app backups

A Google student account is created for every student as part of the enrollment process. These accounts are managed and administered by the School's IT department and are used by students to complete assignments, collaborate with peers and teachers, and build digital citizenship skills.

For further details on how Google uses your children's information, please refer to [Google's Privacy Notice](#).

Google account retention:

Once a student leaves the School, the student will continue to have access to their Google student account for a temporary period after which the account will be deleted:

- Junior School students - 3 months after they leave the School
- Senior School students - 12 months after they leave the School

7 Use of Third-Party Applications and Data Sharing

To support the delivery of education and the effective operation of the school, staff, student, and parent information will be shared with approved third-party applications. These applications are used for essential educational, administrative, and communication purposes.

Data Protection and Security

- The school ensures to the best of its ability that all third-party applications comply with relevant data protection laws and regulations.
- Information shared is limited to what is necessary for the application's intended purpose.
- The school conducts due diligence on third-party vendors to ensure they maintain appropriate security measures to protect personal data.

For further details on how the School uses and shares your personal data, and how you can exercise your data privacy rights, please refer to the School's [Privacy Policy](#).

8 Prohibited Use of VPNs on the School Network

To maintain the integrity, security, and appropriate use of the school's network, the use of Virtual Private Networks (VPNs) by staff and students is strictly prohibited while connected to the school's Wi-Fi or wired network.

Reasons for this restriction:

- Network Security – VPNs can bypass security measures designed to protect users and data.
- Content Filtering – The school uses filtering systems to ensure a safe and appropriate online environment; VPNs can circumvent these protections.
- Compliance – Use of VPNs violates school policies and external regulatory requirements related to online safety and cybersecurity.



Exceptions:

Only approved members of the IT Department are authorized to use school-managed VPNs for site-to-site connectivity and other essential operational purposes. Unauthorized use of VPNs by any other staff or students is strictly prohibited and will result in disciplinary action.

9 AI - Artificial Intelligence

The school recognises both the benefits and risks of AI in education and is committed to its responsible and ethical use. To support this, the school has established a comprehensive AI Use Policy that outlines guiding principles, responsibilities, and integrity while providing clear guidance on AI implementation across learning and operations.

As part of its commitment to AI literacy, the school aims to equip both students and staff with the necessary skills to understand, evaluate, and responsibly use AI. This includes a focus on ethical considerations, data privacy, and safe usage practices to ensure AI enhances learning without compromising security or fairness.

Additionally, the school is dedicated to continuous training and evaluation of AI tools to keep pace with technological advancements, assess their impact, and ensure alignment with educational values. Through ongoing professional development, workshops, and regular reviews, the school fosters an informed and adaptable learning environment.

For more details and to read the full AI Use Policy, click [here](#)

10 Equipment and Digital Content

10.1 Mobile Devices (mobile phones, tablets and other mobile devices)

(Please refer to Mobile Device Acceptable Use – Pupil [ICT-POL-004-S002])

- Mobile devices brought to school are the responsibility of the device owner. The School accepts no responsibility for the loss, theft, damage or insurance of personally-owned mobile devices.
- Mobile devices may not be used in certain areas within the school site, eg changing rooms and toilets. In Isa Town, “Mobile-Free” signs to this effect are displayed.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.

10.2 Pupils’ Use of Personal Devices

- Other than in the Senior School, pupils’ mobile phones must not be brought into school.
- The School accepts that there may be rare, particular circumstances in which a parent of an Infant or Junior child wishes him or her to have a mobile phone available. In these cases, the device will be given to the School Reception during the school day.
- If a pupil breaches this policy, the mobile device will be confiscated and be held in a secure place in school.
- Personal mobile devices will only be used during lessons with permission from the teacher.
- Pupils must not be in possession of phones and/or other devices capable of connecting to the internet or other networks in examinations. Any pupil found in possession of a mobile device during an exam will be reported to the appropriate examining board in accordance with the board’s regulations. This may result in the pupil’s withdrawal from either that examination or all examinations.



- Pupils should only share their phone numbers with trusted friends and family. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- If a pupil needs to contact his or her parents or carers, they should speak to a member of staff. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the School Office.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including, but not limited to: pornographic content; violent content; evidence of bullying; illegal content and material that could harm the School in any way. In the event that the Head of School or Principal has a suspicion that the device has been used inappropriately, the user will unlock the device to allow the device to be inspected.

10.3 Staff Use of Personal Devices (owned by the School or by the Staff Member)

- Staff will be issued with a school phone where contact with pupils, parents or carers is required, for instance for off-site activities, such as overseas trips and field trips.
- Personally owned devices must be securely passcoded.
- Mobile phones and personally owned devices will be in “silent” mode when in lessons, assemblies, meetings etc.
- Photographs or video footage of pupils should ideally only be taken using school equipment for professional purposes authorised by the School. Images should be stored securely on the designated Shared Google Drive (Media Drive).. If personal equipment is used to record images, the images should be uploaded to the School’s system as soon as possible thereafter and deleted from the personal device.
- The School reserves the right to search the content of any devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including, *but not limited to*: pornographic content; violent content; evidence of bullying; illegal content and material that could harm the School in any way. In the event that the Head of School or Principal has a suspicion that the device has been used inappropriately, the user will unlock the device to allow the device to be inspected.

10.4 Digital Images and Video

- Unless highlighting a specific achievement or role, we generally only use first names in online photographs.
- If individual photos of pupils (but not group photos) are used prominently and for an extended period, on the school website, in the prospectus or in other high profile publications, the School will obtain individual parental permission for such use.
- The Digital Safety education programme includes information about how images can be manipulated and emphasises the need to be very careful about placing any personal photos on any “social” or online space.
- Pupils are taught that they should not post images or videos of others without their permission. The risks associated with providing information with images (including the name of the file) that may reveal the identity of others and/or their location are covered in Digital Safety education.

11 Key Responsibilities

11.1 Principal

- Maintain a high level of relevant knowledge of digital safeguarding issues.



DIGITAL SAFETY POLICY - SECTION 1

ICT-POL-004-S001 |v3.0|Effective Mar 2022

- Ensure that the School's procedures for information handling provide for appropriate levels of security and confidentiality.
- Ensure that all staff receive suitable training to carry out their digital safety roles.
- Ensure that Governors are updated annually, or more frequently as necessary, on online safety matters.
- Ensure that the School website includes relevant information relating to digital safety.
- Discuss incident logs with ELT, modifying, if the logs show need, relevant digital safety practices.
- Approve the Digital Safety Policy and ensure that it is monitored in terms of effectiveness and is reviewed annually so that it remains up-to-date with any changes in practice and/or the digital landscape.

11.2 Heads of School

- Maintain a high level of relevant knowledge of digital safeguarding issues.
- Ensure that a "safeguarding culture" exists and is maintained.
- Promote awareness of and commitment to digital safety throughout the school community.
- Take overall responsibility for digital safety in their part of the School.
- Be the first point of contact for anyone wishing to report a serious digital safety incident
- Maintain a log of incidents.
- Be fully conversant with procedures to be followed in the event of a serious digital safety incident.
- Ensure that digital safety education is embedded within the curriculum.

11.3 Director of IT

- Take a leading role in establishing and reviewing the School's Digital Safety Policy.
- Ensure that the School uses appropriate IT systems and software including filtered website/Internet Service.
- Keep ELT up to date with any issues or developments.
- Ensure that staff are aware of the procedures to be followed in the event of a digital safety incident
- Keep up-to-date re online safety issues and UK legislation.
- Ensure that:
 - The school's password policy is strictly adhered to.
 - Systems are in place for misuse detection and malicious attack.
 - The School's web filtering is applied and updated on a regular basis.
- Ensure that digital activity is regularly monitored and that any misuse/attempted misuse is reported immediately to the relevant SLT or DSLs and School Principal.
- Ensure that staff are aware of the procedures to be followed in the event of a digital safety incident and appropriate actions are taken.

11.4 Head of Digital Learning

- Take a leading role in establishing and reviewing the School's Digital Safety Policy.
- Promote, with others, awareness of and commitment to digital safety throughout the school community.
- Report digital safety related issues to the ELT and School Principal.
- Keep ELT up to date with any issues or developments.
- Facilitate training and advice for all staff.
- Keep up-to-date re online safety issues and UK legislation.

11.5 Members of the Board of Governors

- Receive and comment upon reports from the Principal on any digital safety matters



- Direct any parents with questions or concerns to the appropriate Head of School

11.6 Computing Curriculum Subject Leaders

- Oversee the delivery of the digital safety component of the Computing and other subject areas via the Future Ready Curriculum.
- Make recommendations as to developments and possible improvements to this aspect of the digital safety curriculum

11.7 Teachers

- Supervise and guide pupils carefully when engaged in activities involving digital technology (including ECAs)
- Ensure pupils are fully aware of legal and ethical issues relating to electronic content, such as copyright.
- Report suspected or actual misuse or problems to the Head of School or designated SMT member.

11.8 Staff

- Sign and adhere to the Staff AUP, and any updates. The AUP will be signed by new staff on induction.
- Report any suspected or actual misuse or problem to the Head of School.
- Maintain up-to-date knowledge of digital safety policies, issues and guidance.
- Model safe, responsible and professional behaviours in their use of technology.
- At the end of employment, or on demand, return any devices loaned by the School. This will include providing PIN numbers, IDs and passwords to allow devices to be reset.

11.9 Pupils

- Adhere to the Pupil AUP and any additions of modifications thereafter.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Immediately report any actual or suspected misuse of IT facilities and/or digital technologies.
- Take appropriate action if they or someone they know is worried or vulnerable when engaged in digital activity.
- Understand the importance of adopting safe behaviours when using digital technologies out of school.
- Contribute to any school surveys that gather information about their digital experiences.