CANBURY SCHOOL

ONLINE SAFETY POLICY

Last Review Date:	**June 2026**
Policy Owner:	**P Rich, S Harrison**
Approved by:	**L Anindita-Beckman**
Next Review Date:	**June 2027**

Introduction

Key people / dates

Designated Safeguarding Lead (DSL)	Mr Will Rush
Deputy Designated Safeguarding Leads (DDSLs)	Ms Louise Boggi Mrs Kirsty Lansdell
Online-safety lead	Mr Will Rush
Link governor for safeguarding (includes online safety)	Elyse Waites
PSHE/RSE lead	Mr Will Rush
Network/IT manager	Mr Simon Harrison
Date this policy was reviewed and by whom	June 2026
Date of next review and by whom	June 2027

Contents

Introduction 2
Key people / dates 2
Contents 2
Overview 4
1. Aims 4
2. Further Help and Support 4
3. Scope 4
4. Legislation and guidance 5
5. Roles and responsibilities 5
All staff 5
Head – Mrs P Rich 6
Designated Safeguarding Lead / Online Safety Lead – Mr Will Rush 6
Governing Body, led by Safeguarding/Pastoral Link Governor – Ms Elyse Waites 7
PSHE / RSE Lead – Mr Will Rush 8
Computing Teachers – Mr Sy Hussain 9
Subject teachers 9
IT/Network Manager – Mr Simon Harrison 9
Chief Privacy Officer – Ms Lusia Anindita-Beckman 10
Visitors and members of the community 10
Students 10

Parents/carers 11
6. Educating students about online safety 11
7. Educating parents/carers about online safety 12
8. Online Bullying / Cyberbullying 13
8.1 Definition 13
8.2 Preventing and addressing cyber-bullying 13
8.3 Examining electronic devices 14
8.4 Artificial intelligence (AI) 14
9. Acceptable use of the internet in school 14
10. Personal devices, including wearable technology and school managed Chromebooks 14
10.1 Chromebooks 14
10.2 Students using mobile devices in school 15
10.3. Staff using work devices in and out of school 15
10.4 Adult personal mobile devices 16
10.5 Network / internet access on school devices 16
10.6 Trips / events away from school 17
11. Appropriate filtering and monitoring 17
12. Electronic communications 17
12.1 Email 17
12.2 Digital images and video 18
13. Social media 19
13.1 Canbury School's SM presence 19
13.2 Staff, students and parents' SM presence and usage 19
14. Handling online-safety concerns and incidents 21
15. Privacy, Searching and Confiscation 22
16. Reasonable adjustments for students with SEND 22
17. Training 22
18. Complaints 23
Appendix 1 – Related Policies and Documents 24
Appendix 2 – Procedures linked to misuse of mobile phones/devices 24
Appendix 3 – Acceptable Use Of The School's ICT Systems And Internet: Agreement For Staff, Governors, Volunteers And Visitors 27
Appendix 4 – Acceptable Use Of The School's ICT Systems And Internet: Agreement For students And Parents/Carers 28
Appendix 5 – Online safety training needs – self-audit for staff 30

Overview

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purpose
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with our Safeguarding Policy.

The DSL will handle referrals to local authority Single Point of Access (SPA) or multi-agency safeguarding hubs (MASH) and normally the Head will handle referrals to the LA designated officer (LADO).

3. Scope

This policy applies to all members of the Canbury School community (including teaching and support staff, supply teachers, peripatetic teachers, governors, volunteers, contractors, students, parents/carers and visitors) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Links to other policies and procedures:

- Safeguarding Incident log on MyConcern

- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Acceptable Use Policies (AUPs) for Students/Parents and Carers / Staff, Volunteers Governors & Contractors

4. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Digital and Technology Standards
- Mobile phones in school

It also refers to the DfE's guidance on protecting children from radicalisation and The Independent School Standards Guidance for Independent Schools April 2026, para 3.21-3.23 standard 9.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, Children's Wellbeing and Schools Act 2026 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

5. Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school. We learn together, make honest mistakes together, and support each other in a world that is online and offline at the same time.

All staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- Reading, adhering to and helping to promote this policy in conjunction with the school's main safeguarding policy and the relevant parts of Keeping Children Safe in Education
- Understand that online safety is a core part of safeguarding and part of everyone's job
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (AUP), and ensuring that students follow the school's terms on acceptable use
- Know who the Designated Safeguarding Lead (DSL) / Online Safety Lead (OSL) is (Mr Will Rush) notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by alerting them via MyConcern
- Following strict authorisation protocols if an online restriction must be temporarily modified for valid educational purposes. Staff are prohibited from requesting technical bypasses directly from the IT department; instead, a formal request detailing the educational rationale and prospective digital assets must be submitted to the Designated Safeguarding Lead (DSL) for safeguarding triage. Technical modifications or filtering exceptions will only be implemented by the Network Manager following explicit, written sign-off from the DSL, ensuring an auditable oversight trail.
- Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHE/RSE curriculum, both outside the classroom and within the curriculum
- Have an up-to-date awareness of a range of online safety issues and how they may be experienced by the children in their care
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites
- Carefully supervise and guide students when engaged in learning activities involving online technology
- Model safe, responsible and professional behaviours in their own use of technology
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues.

This list is not intended to be exhaustive.

Head – Mrs P Rich

Key responsibilities:

- Has overall responsibility for Canbury School's online safety provision by ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Liaise with the designated safeguarding lead on all online-safety issues and receive regular updates
- Ensure the DSL works with colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Ensure the school implements and makes effective use of appropriate ICT systems and services
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively

- Assigning responsibility to a trained member of staff to conduct regulated online searches and digital background checks on all shortlisted candidates as an integrated element of our safer recruitment due diligence. In strict alignment with Keeping Children Safe in Education parameters, these targeted searches are executed solely to identify substantiated incidents, behavioral alerts, or regulatory concerns that are publicly available online, providing a transparent foundation for the panel to explore relevant disclosures directly with the applicant during the interview stage.
- Ensure the school website meets statutory requirements.

This list is not intended to be exhaustive.

Designated Safeguarding Lead / Online Safety Lead – Mr Will Rush

Full details of the school's designated safeguarding lead (DSL) and deputies roles are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head and safeguarding governor to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Head, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour and anti-bullying policy
- Working with the school's IT manager to ensure that staff have up-to-date training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSE guidance and beyond, in wider school life

This list is not intended to be exhaustive.

Governing Body, led by Safeguarding/Pastoral Link Governor – Ms Elyse Waites

The governing board has overall responsibility for monitoring this policy and holding the Head to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Ms Elyse Waites.

All governors will:

- Ensure they have read and understand this policy
- Ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of DSL
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (AUP)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

This list is not intended to be exhaustive.

PSHE / RSE Lead – Mr Will Rush

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) education curriculum.
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way
- Work closely with all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE
- Ensure that the RSE policy is included on the school website
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

This list is not intended to be exhaustive.

Computing Teachers – Mr Sy Hussain

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

This list is not intended to be exhaustive.

Subject teachers

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSE curriculum, and model positive attitudes and approaches to staff and students alike
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.

This list is not intended to be exhaustive.

IT/Network Manager – Mr Simon Harrison

The ICT manager is responsible for:

- As listed in the 'all staff' section, plus:
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Collaborating regularly with the DSL and leadership team to help them make key strategic decisions around the online safety/safeguarding elements of technology
- Support the DSL and SLT to carry out an annual online safety audit
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.
- To report online-safety related issues that come to their attention in line with school policy

This list is not intended to be exhaustive.

Chief Privacy Officer – Ms Lusia Anindita-Beckman

Key responsibilities:

- Work with the DSL, Head and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- Providing privacy advice relating to matters such as the handling of personal information
- Co-ordinating the School's response to suspected or confirmed data breaches
- Maintaining a record of the personal information that the School holds, and how it is secured
- Completing or coordinating privacy audits or other assurance activities at the School to ensure that it meets privacy obligations
- Responsible for the School's privacy notices and policies
- Reviewing existing or proposed arrangements with contracted service providers (CSPs) and providing recommendations to clarify privacy responsibilities
- Coordinating privacy training, and other activities to promote privacy awareness for all staff and students
- Responding to queries about the School's privacy practices from members of the public
- Handling privacy complaints that the School receives directly
- Liaising with ICO about data breach notifications, privacy complaints or significant projects
- Assessing whether requests from other organisations to share personal information that the School holds are permitted under GDPR.

This list is not intended to be exhaustive.

Visitors and members of the community

Key responsibilities:

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (AUP).

Students

Key responsibilities:

- Read, understand, sign and adhere to the student acceptable use policy
- Treat home remote learning in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Respect the feelings and rights of others both on and offline, in and out of school
- Take responsibility for keeping themselves and others safe online
- Report to a trusted adult, if there is a concern online.

Parents/carers

Parents/carers are expected to:

- Read, sign and promote the school's student/parent/carer acceptable use policy (AUP) and encourage their children to follow it
- Notify a member of staff or the Head of any concerns or queries regarding this policy
- Talk to the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre
Hot topics – Childnet
Parent resource sheet – Childnet

6. Educating students about online safety

It is important that we in school establish a carefully sequenced curriculum for online safety that builds on what students have already learned and identifies subject content that is appropriate for their stage of development.

The following subjects have the clearest online safety links:

- Personal, Social, Health and Economic Education (PSHE)
- Relationships and Sex education, (RSE)
- ICT

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum and making the most of unexpected learning opportunities as they arise (which have a unique value for students).

Students will be taught about online safety as part of the curriculum:

In **KS3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (ask the DSL what appropriate filtering and monitoring policies are in place if you are unsure).

Equally, all staff should carefully supervise and guide students when engaged in learning activities involving online technology (including, extracurricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation, conspiracy theories and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

7. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in emails, coffee mornings or other communications home, and in information via our website. This policy will also be shared with parents/carers via our website.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head.

8. Online Bullying / Cyberbullying

8.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour and anti-bullying policies.)

8.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8.3 Examining electronic devices

The Head, and any member of staff authorised to do so by the Head, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting.

For full details on this, please refer to our Searching and confiscation policy.

8.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Canbury School recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Canbury School will treat any use of AI to bully students in line with our anti-bullying and behaviour policies.

All AI tools used in the school, whether by staff or students, must satisfy the Department for Education's Generative AI: Product Safety Expectations, including robust filtering and monitoring, safeguards against misuse, logging and data protection. Generative AI: product safety expectations - GOV.UK

Students with Special Educational Needs and Disabilities (SEND) shall be supported to use AI tools safely and meaningfully; tools should be selected for accessibility, clarity and fairness, and staff will scaffold their use to avoid potential harm or misunderstanding.

Our Sixth Form students will receive dedicated support and instruction in the ethical and effective use of Artificial Intelligence (AI) tools. Recognising that AI is an increasingly integral part of higher

education and the modern workplace, our approach is designed to equip students with the critical skills necessary to navigate this technology responsibly.

Staff must not feed confidential personal or sensitive student's data into any AI tool without prior consent and vetting of the vendor's data protection and security practices. All user data within Google Workspace for Education, including data from NotebookLM and Gemini, is kept separate from Google's general AI training models. Therefore, staff have been advised to use these tools when accessing AI support.

Staff should be aware of the risks of using AI tools whilst they are still being developed.

9. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. It will be necessary to reinforce these agreements at the beginning of any school year, but also to remind students that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

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

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

The school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

More information is set out in the acceptable use agreements in the appendix.

10. Personal devices, including wearable technology and school managed Chromebooks

10.1 Chromebooks

- From September 2019 new students were required to purchase a managed Chromebook for use in lessons and at home. From September 2022 the school is providing new students (and existing students who need a replacement device) with school-owned Chromebooks on long term loan. Each issued device remains the responsibility of the student in the case of loss or damage, but remains the property of Canbury School.
- Chromebooks assigned to students and staff must have a password so that unauthorised people cannot access the content. When a device is not being used, you should ensure that it is locked or that you are logged out to prevent unauthorised access.

10.2 Students using mobile devices in school

The school will not accept liability for the safekeeping of mobile phones/devices which will remain the responsibility of the student at all times, unless they have been handed in to Reception staff for safekeeping. Only in exceptional circumstances (usually involving other breaches of our code of conduct) would the school investigate the theft or loss of a mobile phones/devices.

Please read the following in conjunction with acceptable use policies and the following sections of this document.

- **Students in Year 7 to 13** are allowed to bring mobile phones, but these must be kept in their designated Yondr pouch for the entirety of the day. These can be kept in a safe space by the student, such as their locker or school bag.
- **Students in Year 12 and 13** are allowed to use their mobile phones during break and lunch, but only in the 6th form common room. Between these times, phones are off and kept in their designated Yondr pouch.

Any attempt to use a phone in lessons without permission or to take illicit photographs/videos or purposefully not kept in their Yondr pouch will lead to the application of proportionate consequences, including temporary confiscation

Important messages and phone calls to or from parents/carers can be made at the school office, who will also pass on messages from parents to students in emergencies

Personal telephone numbers may not be shared with students or parents/carers and under no circumstances may staff contact a student or parent/carer from a personal telephone number.

The Head and authorised staff have statutory powers to search a student or their possessions (including a mobile phone) if they have reasonable grounds to suspect the student possesses a prohibited item or an item banned under school rules.

See appendix 2 for details of the "Procedures linked to misuse of mobile phones/devices"

10.3. Staff using work devices in and out of school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in the staff AUP

Staff are required to use two-factor authentication (2FA or multi-factor authentication, MFA) for their Google Workspace accounts and are encouraged to use 2FA / MFA for all services and subscriptions that support it.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Manager.

10.4 Adult personal mobile devices

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours.

- If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with reception to answer on their behalf or ask for the message to be left with the school office

Volunteers, contractors, governors should leave their phones in their pockets and turned off.

- If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Head should be sought (the Head may choose to delegate this) and this should be done in the presence of a member of staff

Parents are asked to leave their phones in their pockets and turned off when they are on site.

- When at school events, please refer to the Digital images and video section of this document on page.

Parents are asked not to call students on their mobile phones during the school day; urgent messages can be passed to a child via reception.

10.5 Network / internet access on school devices

- **Students** are allowed to access the school wireless internet network for school-related internet use / limited personal. All such use is monitored.
- **Students** are issued with a managed Google Workspace for Education
    - It is provided to support each student's learning and must only be used for school work and activities.
    - Their use of this services is monitored.
- **Students** must report any accidental access to materials of a violent or sexual nature directly to the Online Safety Coordinator.
    - Deliberate access to any inappropriate materials by a student will lead to the incident being recorded and will be dealt with under the school's Behaviour Policy.
- **Teaching staff** are issued with a managed Google Workspace for Education.
    - It is provided to support school work and activities. The account is not to be used for personal or leisure activities, and its use is audited and can be monitored

- **All staff** must not access any website or personal email which is unconnected with school work or business from school devices whilst teaching or in front of students. Such access may only be made in staff-only areas of school.
- **All staff** should take precautions against threats to school data
- **All staff** must immediately report to the Online Safety Coordinator the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- **Volunteers, contractors, governors** can access the wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices.

10.6 Trips / events away from school

For school trips/events away from school, teachers will be issued a school phone and this number used for any authorised or emergency communications with students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher.

Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

11. Appropriate filtering and monitoring

In accordance with the mandatory parameters set forth in the DfE Digital and Technology Standards, the Governing Body ensures that the school's network infrastructure satisfies the four core filtering and monitoring standards:

1. Assigned Governance: Leadership has established defined operational roles, with the Governing Body holding strategic accountability, the DSL holding safeguarding oversight, and the Network Manager managing technical execution.

2. Statutory Annual Review: The efficacy, blocklists, and keyword logs of our digital tracking software are formally audited and updated at least annually by the DSL and Network Manager to counter emerging threats.

3. Harm Mitigation and Active Blocking: The school maintains automated system filters that completely block illegal or harmful material across the core risk matrices (including CSAM, terrorist, and extremist content) on all school networks and loaned devices.

4. Proactive Monitoring Strategy: Rather than relying solely on physical classroom presence, the school implements automated monitoring software that generates real-time telemetry and safety flags for concerning digital behavior or search triggers. These alerts feed directly into the DSL's dashboard to support immediate intervention, while technical parameters are adjusted carefully to prevent 'over-blocking' from restricting access to our preventative online safety curriculum.

At home, school devices are also filtered and monitored. Additionally, when students log into any school system on a personal device, activity may also be monitored.

12. Electronic communications

Please read this section alongside references to student-staff communications in the staff code of conduct, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

12.1 Email

Students and staff at this school use Gmail for all school emails. This system is integral to Google Workspace for Education's identity and access management system and is fully auditable, trackable and managed by our school's IT manager. This is for the mutual protection and privacy of all staff, students and parents, as well as to support data protection.

General principles for email use are as follows:

- School systems are the only means of electronic communication to be used between staff and students / staff and parents/carers (in both directions).
- There should be no circumstances where a private email is used.
- If sensitive data needs to be shared with external agencies, Egress systems must be used
- Internally, staff should use Google Drive for file sharing
- Appropriate behaviour is expected at all times, and be professional in tone and content.
- Students and staff should not use their school email account for personal use.

See also the social media section of this policy.

12.2 Digital images and video

When a student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

In absolute compliance with statutory safer recruitment and data protection frameworks, members of staff are strictly prohibited from using personal mobile devices, personal smart technology, or personal cameras to capture photographs, audio, or video recordings of registered students under any circumstances. All digital imagery or media documentation relating to school curriculum tasks, sports fixtures, or off-site educational visits must be captured exclusively on school-owned, school-managed, and securely encrypted hardware. Breach of this mandate represents a serious violation of the Staff Code of Conduct and will trigger immediate disciplinary investigation.

When taking photographs in School, staff must:-

- Only take photographs and videos of children with their parents/carers permission (provided and signed for via the parent contract)
- Have been designated to take photographs or video before doing so
- Never use any image or video that might embarrass or humiliate. Staff must only use images of students who are appropriately dressed. They should be particularly careful when taking images or videos of students swimming or doing sports
- Be clear about the purpose of the activity and what will happen to the photographs when the lesson/activity is concluded
- Ensure that photographs are taken for valid educational purposes and, if in doubt, consult with a member of the SLT.

- Ensure that classroom cameras are not utilized to broadcast lessons or facilitate remote connectivity without explicit prior authorization from the Designated Safeguarding Lead (DSL), and that any captures are strictly limited to the teacher and the smart board.

Parents / carers

Parents/ carers are welcome to take photographs of (and where appropriate, film) their own children taking part in sporting and outdoor events, and in other School events, subject to the following guidelines:-

- When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others
- We ask parents not to take photographs of other students (except incidentally as part of a group shot) without the prior agreement of that student's parents
- Parents are reminded that such images are for personal use only. Images which may identify other students should not be made accessible to others via the Internet (for example, on Facebook or Instagram), or published in any other way
- Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; we therefore ask that it is used with consideration at indoor events
- Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts
- Parents may not film or take photographs in changing rooms or backstage during School productions, nor in any other circumstances, in which photography or filming may embarrass or upset students
- The School reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally).

Students

- Must not take photographs or make recordings of other students unless expressly authorised by a member of staff and this will only be granted for School activities such as, a photo shoot in Photography or photographs of a School fundraising event.

Please the Taking, storing and using images of students policy for further information.

13. Social media

13.1 Canbury School's SM presence

Canbury School works on the principle that if we don't manage our social media reputation, someone else will.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

The Senior Leadership Team & Pastoral administrator is responsible for managing our Instagram and other social media accounts and checking our Wikipedia and Google reviews.

Any social media accounts (including blogs, forums, twitter, YouTube, etc.), sites or pages used or set up for the purpose of furthering the School's business or facilitating the provision of the curriculum to its students must be pre-approved by the Head, shall remain the property of the School and the Head must have access to it.

13.2 Staff, students and parents' SM presence and usage

Breaches will be dealt with in line with the school behaviour policy (for students) or code of conduct for staff.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Canbury School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and students will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave positively, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed.

We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when.

Email is the swiftest electronic communication channel between parents and the school, and between staff and students.

Students are not allowed* to be 'friends' with or make a friend request to any staff, governors, volunteers and contractors or otherwise communicate via social media.**

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the student or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head (if by a staff member).

Staff are reminded they:

- Are obliged not to bring the school or profession into disrepute, and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online
- Must never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school thus bringing the school into disrepute
- Must obtain the prior written approval of the Head to the wording of any personal profile which you intend to create where the School is named or mentioned on a social networking site
- Must report to the Head immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School
- Must not use social networking sites as part of the educational process, e.g. as a way of reminding students about essay titles and deadlines
- Must immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other School policy
- Must not provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the School and create legal liability for both the author of the reference and the School
- Must not use commentary deemed to be defamatory, obscene, proprietary or libellous
- Must not circulate or post commercial, personal, religious or political solicitations or promotion of outside organisations unrelated to the school
- Must not use their work email address for any personal use of social media
- Must amend any personal profiles on social networking sites once you are no longer employed or associated with our School
- Must provide to the Head any relevant passwords and other information to allow access to any social media site, page or account which has been used or set up for the purpose of furthering the School's business or facilitating the provision of its curriculum and will relinquish any authority they may have to manage or administer any such site, page or account
- Should be aware that professional contacts that you may have made through the course of employment with us belong to our School, regardless of whether you have made social media connections with them
- Should consider whether a particular posting puts their effectiveness as a teacher at risk
- Should post only what they want the world to see.

Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy. All social media sites are blocked when using the School's Wi-Fi.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

14. Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of ICT and PSHE/RSE).

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in the following policies:

- Child Safeguarding Policy
- Anti-Bullying Policy

- Behaviour Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statements and consent forms for data sharing, image use etc)

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

General concerns must be handled in the same way as any other safeguarding concern.

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

Any concern/allegation about staff misuse is always referred directly to the Head, unless the concern is about the Head, in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline if they wish to seek further advice.

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly serious or breaks the law.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Online Safety Coordinator, data protection officer and the IT Consultant.

15. Privacy, Searching and Confiscation

Full details of the school's search procedures are available in school's Searching and confiscation procedure.

The contents of our IT resources and communications systems are our property. Therefore, those using our equipment, such as wifi and hardware, should have no expectation of privacy.

We reserve the right to monitor, store, intercept and review, without further notice, activities using our IT resources and communications systems.

Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the School.

16. Reasonable adjustments for students with SEND

The school recognises its legal duty under the Equality Act 2010 to prevent students with a protected characteristic from being at a disadvantage. Consequently, our approach to challenging behaviour may be differentiated to cater to the needs of the student. Staff must reflect, evaluate their own practice and seek supervision (SLT and/or the Behaviour Specialist) when working with students who have SEND and/or working with students who display behaviours that challenge.

The School's special educational needs co-ordinator, Deputy Head Pastoral and/or Behaviour Specialist will evaluate a student who exhibits challenging behaviour to determine whether they have any underlying needs that are not currently being met.

Where necessary, support and advice will also be sought from the Mental Health Lead, educational psychologists, medical practitioners, Child Services and/or others, to identify or support specific needs.

When acute needs are identified in a student, we will liaise with external agencies and plan support programmes for that child via the development of a Positive Behaviour Support Plan. We will work with parents, students and staff to create this plan and review it on a regular basis.

17. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

18. Complaints

As with all issues of safety at Canbury School, if a member of staff, a student or a parent / carer has a complaint or concern relating to online safety, prompt action will be taken to deal with it.

Complaints should be addressed to the Online Safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and any members of staff or students involved. Please see the Complaints Procedure for further information.

Incidents of or concerns around online safety will be reported to the school's Online Safety Co-ordinator / Designated Safeguarding Lead in accordance with the school's Child Safeguarding Policy and Procedures and logged.

Appendix 1 – Related Policies and Documents

1. Safeguarding Incident log on MyConcern
2. Safeguarding Policy
3. Behaviour Policy
4. Anti-Bullying Policy
5. Staff Code of Conduct
6. Acceptable Use Policies (AUPs) for:
    - Students/Parents and Carers
    - Staff, Volunteers Governors & Contractors
7. Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
8. Working together to safeguard children (DfE)
9. Searching, screening and confiscation advice (DfE)
10. Sharing nudes and semi-nudes guidance from UKCIS:
    - How to respond to an incident - overview for all staff
    - Full guidance for school DSLs
    - Online Safety Audit for Trainee (ITT) & Newly Qualified Teachers (NQT)
11. Prevent Duty Guidance for Schools (DfE and Home Office documents)
12. Data protection policy
13. Preventing and tackling bullying (DfE)

14. Ofsted Review of sexual abuse in schools and colleges
15. Taking, storing and using images of students policy

Appendix 2 – Procedures linked to misuse of mobile phones/devices

Common Situations and Typical Responses – including consequences

1. A student is caught in possession of a mobile phone/device / A student's mobile phones/devices rings during a lesson.

- In the first instance, the student will be asked to turn off their phone/put their phone away. If it happens again, the teacher will confiscate the mobile phones/device, which will be kept for safekeeping in reception. The student can collect the mobile phones/devices at the end of the day. If this keeps occurring, a sanction will be given and/ or parents will be contacted.

2. Without authorisation, a student uses the mobile phones/devices to communicate with a parent or other person in response to a situation at school.

- Typically, this might involve a call to a parent to complain about an incident in school. This is wholly unacceptable, as it circumvents the school's clear procedures for dealing with any behaviour or other incident in school. It would often mean that the parent is contacted by an upset child and provided with a distorted or inappropriate interpretation of what has transpired – sometimes leading to an angry or misinformed response from the parent.

- Similarly, it is not permitted that students telephone home to inform parents that they are unwell and need to be collected from school. If a student is unwell and feels they need to go home, they should ask a member of staff to call from reception.
- The student and parent will be reminded to the above procedures.

3. A student records an unauthorised picture or video clip of a student.

- The student will be told to delete the image/file from their phone (including any cloud storage system). The teacher will confiscate the mobile phone/device, which will be kept in safekeeping in reception. The student will have a meeting with the Head or another member of the SLT team to discuss the incident. The incident will be recorded and parents/carers will be contacted. The student can collect the mobile phone/device at the end of the day.

- Should it be discovered that the student has posted such images/video clips on the internet (for example, via YouTube) or has transferred it electronically to other digital device, then a fixed term suspension will be considered. The reprimand will be even more severe if, for example, investigations show the action to be malicious and/or part of a wider bullying or intimidation campaign or the behaviour has been repeated.

4. Sharing of nudes and semi-nudes.

- Nudes and semi-nudes can be shared by, and between, children and young people under a wide range of circumstances and are often not sexually or criminally motivated. The School's response to an incident will differ depending on the motivations behind the incident and the appropriateness of the child or young person's/people's behaviour. See the section on Sharing of nudes and semi-nudes in the Child Safeguarding Policy.

- Should it be discovered that a student has posted or shared such images the situation will be assessed: Responding to incidents of sharing nudes and semi-nudes is complex because of its legal status. Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes imagery of yourself if you are under 18.

5. A student records an unauthorised picture or video clip of a teacher or other member of staff.

- A fixed term suspension will be considered and parents/carers will be asked to attend school to discuss methods of preventing further misuse and to collect the mobile phone/device following confiscation. The student will be told to delete the image/file from their phone (including any cloud storage system) in the presence of their parent/carer.

- Should it be discovered that the student has posted such images/video clips on the internet (for example, via YouTube) or has transferred them electronically to other digital device, they would possibly face a more severe reprimand. For example, the action was investigated and considered to be repeated or malicious or that such images/clips were damaging to the good reputation or professional standing of the individual teacher and/or Canbury School.

- It should be noted that the member of staff concerned might take further independent action, perhaps following consultation with their professional association.

6. Inappropriate text messages, email or any other form of electronic communication are sent by a student (including messages of a threatening or bullying nature).

- The context and nature of the messages sent will be crucial in determining the severity of the response. For example, if the messaging is repeated behaviour or part of a wider bullying campaign, this will be treated very seriously and the sanctions are likely to include a fixed term suspension or even permanent exclusion (please refer to our Anti bullying policy and the Behaviour Policy). As above, parents/carers will typically be invited to school to collect the confiscated mobile phone/device and to discuss ways of preventing similar unacceptable behaviour in the future.

- At all times, the school will consider each set of circumstances on a case-by-case basis before determining a course of action or applying proportionate responses.

As with all policies at Canbury School, we welcome feedback from students and parents and are constantly striving to improve our procedures in order to ensure good order, student safety and happiness within our inclusive community.

Appendix 3 – Acceptable Use Of The School's ICT Systems And Internet:
Agreement For Staff, Governors, Volunteers And Visitors

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- **Access or Share Inappropriate Content:** Access, create, store, share, or send material that is illegal, pornographic, offensive, obscene, or otherwise harmful. This includes content of a violent, discriminatory, extremist, or radicalised nature. Access social networking sites or chat rooms.
- **Compromise Safeguarding:** Take or share photographs or videos of students without following checking permissions first on Satchel One. Do not accept "friend" requests from students on social media, give out your personal contact information, or engage in private messaging with students through personal accounts. Share confidential information about the school, its students or staff, or other members of the community.
- **Harm the School's Reputation:** Engage in any activity, including on personal social media, that could defame or disparage the school, its staff, or students, or bring the school into disrepute.
- **Breach Security:** Share your password or login details with anyone. You will not attempt to gain unauthorised access, modify or share any network areas, accounts, or files, or use websites or other mechanisms to bypass the school's filtering or monitoring systems. Transfer or store personal or confidential data from Canbury ICT systems onto a personal device such as a USB flash drive, home computer, private e-mail or personal online storage.
- **Misuse School Property:** Connect any unauthorised devices to the school network or install any unauthorised software/apps. Do not cause intentional damage to equipment, or remove, delete, or dispose of school ICT systems or data without permission.
- **Engage in Misconduct:** Use school systems for illegal activities such as online gambling, phishing, or financial scams. Do not use your position to promote a private business unless it is directly related to the school. Use any improper language when communicating online, including in emails or other messaging services

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will:

- **Use Systems Professionally and Appropriately:** Use all school ICT facilities, devices, and internet access responsibly and solely for educational or work purposes.
- **Adhere to Procedures:** Accept that the school monitors your ICT usage for safeguarding and security purposes. You will not install software or subscribe to online services without explicit authorisation from the Bursar. Accept that apps and services purchased by the school are its property.
- **Maintain Security:** Secure all school-owned devices and confidential data when used outside of school. This includes using strong passwords and multifactor authentication where available.
- **Report Concerns**: Immediately report any concerning material or activity you or a student find to the Designated Safeguarding Lead (DSL) and ICT manager.
- **Manage Data Responsibly:** Use only school-provided systems for electronic communication with parents/carers and students. Do not transfer or store confidential data onto personal devices (e.g., USB drives, personal computers) unless it is securely encrypted and authorised.

- **Use Personal Devices Responsibly:** This must be within policy guidelines. Accept that the school isn't liable for any damage or loss to personal devices or apps. Personal app purchases are non-transferable, non-reimbursable, and require Bursar approval for school use
- **Respect Copyright:** Adhere to all copyright laws and intellectual property rights.

This is not an exhaustive list. The Head will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

I understand this forms part of the terms and conditions set out in my contract of employment and that failure to comply with this agreement can lead to disciplinary action.

Signed (staff member/governor/volunteer/visitor):

Name: **Date:**

Appendix 4: Acceptable Use Of The School's ICT Systems And Internet: Agreement For students And Parents/Carers

As a student of Canbury School, I understand that:

- Canbury School ICT facilities support my learning and the school operations
- Use of these facilities come with responsibilities
- This Acceptable Use Procedure (AUP) outlines my ICT responsibilities
- Online safety is part of the curriculum and this AUP
- School rules apply to ICT use
- Misuse of ICT systems and service may lead to school disciplinary action or if laws have been broken, the matter will be referred to the relevant authorities, including the police.

I will read this AUP carefully with my parents/carers. I must sign the declaration with my parents/carers to receive a personal user account. Furthermore, I will use ICT facilities responsibly and legally.

I will (Do):

Personal Safety & Reporting:

- Keep my usernames, passwords, and other private information safe. I will not share them with anyone, including my name, address, or phone number, without a teacher's or parent's permission.
- Immediately tell a teacher or another adult if I find any material that upsets, distresses, or harms me or others.
- Report any concerning or inappropriate content or abusive language directed at me to a staff member or Mr. Rush/DSL.

General Conduct:

- Use the school's ICT systems and the internet responsibly and only for educational purposes.
- Use only my designated school Gmail account.
- Use appropriate language and not bully or harass others online.

- Respect the privacy of others. I will not share their personal information online without their consent.

Chromebook & Equipment:

- Always look after my Chromebook and ensure I don't leave it unattended.
- Bring my Chromebook to school fully charged every day.
- Always log off or shut down a computer when I've finished using it.

I will not (Don't):

Forbidden Online Activities:

- Access any inappropriate websites, social media sites, chat rooms, or gaming sites unless a teacher has expressly allowed it for a learning activity.
- Use the internet to bully, harass, or discriminate against someone else.
- Create, share, or view any material that is pornographic, offensive, obscene, or otherwise inappropriate.
- Share personal information about myself or others online.
- Access or use AI tools like ChatGPT to complete assessments or assignments and present the work as my own.
- Use valuable school time accessing non-educational games or sites.

Security & Integrity:

- Open email attachments or follow links in emails without checking with a teacher first.
- Log in to the school's network using someone else's details.
- Bypass the internet filter or search for offensive content.
- Download, share, or use copyrighted materials without permission.
- Commit plagiarism. I will properly cite all sources and clearly indicate direct quotes.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

Misuse of Equipment & Property:

- Attempt to change any settings or install software on school computers or Chromebooks.
- Bring or use hacking tools to access or disrupt the school's IT systems.
- Intentionally damage IT equipment. I will report any damage I know about to the Site Manager or Pastoral Assistant Head and not share this information with other students.
- Take or edit photos or videos of staff or students without their consent.
- Record live video lessons or calls without permission.
- Take part in any online activity that harms the school's reputation.

If I bring a personal mobile phone or other personal electronic device into school:

All students

I will not use a mobile phone or personal device during school time or other activities organised by the school, without a teacher's permission. I will secure my mobile phone in my Yondr pouch during school hours.

I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online.

I agree that the school will monitor my internet use.

This is not an exhaustive list. The Head will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

If I violate this agreement, I may lose Internet and computer access for a period decided by the Head and face further disciplinary action. Each case will be considered individually.

I have read this document and I agree to follow these rules and to support the safe and responsible use of ICT at Canbury School.

Student Signature: …… Year Group: ……..……

Student Name: ……

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Parent/Carer Signature: …… Name: ……..……..……

Appendix 5 – Online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	