Collège Français Bilingue de Londres

("CFBL" or the "School" or “we”)

Online Safety and Use of Internet, Mobile Phones and Other Electronic Equipment Policy (for pupils)

Authorised by:	The Board of Governors of CFBL
On:	WR 26.06.26
frequency of review:	Annually or sooner following any updates to national and local guidance and procedures
Next scheduled review:	June 2027
Circulation:	Governors/all staff/volunteers, automatically; Staff: Shared drive > Policies Parents: on request/School Website

1. Introduction

The digital revolution presents a dual reality for our students: unparalleled access to information and learning tools, alongside the potential for exposure to online risks. Our Online Safety Policy is designed with a dual focus: to cultivate the vast benefits of the internet and to safeguard against its challenges, framed by the "4 Cs" of online safety—Content, Contact, Conduct, and Commerce.

Our Objectives:

- Content: To protect students from exposure to harmful and inappropriate material.
- Contact: To prevent harmful online interactions, including cyberbullying and exploitation.
- Conduct: To educate on the importance of responsible online behaviour and digital citizenship.
- Commerce: To inform about online commercial risks, such as scams and phishing.

In partnership with students, parents*, and staff, we strive to create a digital environment that supports safety, education, and empowerment. This Policy sets forth clear guidelines for online behaviour, the responsible use of technology, and the role of personal devices within our School.

As we navigate the complexities of the digital world, our commitment is not only to provide immediate protection but also to instil lifelong e-safety skills. Through this Policy, we pledge to nurture a digitally savvy community where each student can confidently and ethically engage with technology.

**In this Policy, reference to parents means parents, carers or guardians.*

2. Online Safety

It is the duty of the School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and subtler risks to young people. To address these evolving challenges, the School undertakes an annual review of our online safety approach, supported by a thorough risk assessment that reflects the specific risks our students may face. This process is integral to our commitment to teach pupils to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse, radicalisation and terrorism.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used at School include:

- Websites and applications (such as Google Classroom, Zoom, Pronote, Projet Voltaire, Kwyk);

- Email and instant messaging;
- Social networking sites;
- Music / video downloads;
- Video calls and classes;
- Podcasting;
- Mobile internet devices such as tablets and Chromebooks and including all electronic devices with imaging and sharing capabilities.

This Policy is implemented to protect the interests and safety of our pupils individually and of the whole School community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following School policies:

- Child Protection and Safeguarding Policy;
- Behaviour and Discipline Policy;
- Anti-Bullying Policy;
- Use of Internet, Email & System Policy and Social Media Policy (for staff) ;
- Staff Behaviour Policy;
- CFBL Technology Charter *(Charte informatique*) (for pupils);
- CFBL Acceptable Use Policy for Primary/Secondary School Pupils;
- General Privacy Notice (for all School community);
- Privacy Notice (for pupils aged 13 +);
- Privacy Notice (for staff);
- PSHE / RSHE curriculum documentation;
- Taking Storing and Using Images of Children Policy.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At CFBL, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical-thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

This Policy, th*e CFBL Technology Charter* (for pupils) and the Use of Telephone, Email Systems & Internet Policy & Social Media Policy (for staff) cover both fixed and mobile internet devices provided by the School (such as PCs, laptops, digital cameras, tablets, interactive boards, digital video equipment, mobile phones, including all electronic devices with imaging and sharing capabilities etc.) as well as all devices owned by pupils and staff brought onto School premises (personal laptops, tablets, smart phones, etc.).

CFBL acknowledges its duty under section 26 of the Counter-Terrorism and Security Act 2015 ("the CTSA 2015") to have "due regard to the need to prevent people from being drawn into terrorism", including in the digital world. Guidance on radicalisation, extremism and the Prevent duty are set out in CFBL's Safeguarding and Child Protection Policy.

3. Roles and responsibilities

The Senior Management Team has responsibility for ensuring this Policy is upheld by all members of the School community. They will keep up to date on current e-safety issues and guidance issued by organisations such as CEOP, Childnet International, the Department for Education, the UK Safer Internet Centre and the Camden Safeguarding Children Partnership. As with all issues of safety at the School, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

CFBL believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of School. We keep parents informed about online safety issues.

of e-safety issues.The School recognises that internet safety is a child protection and general safeguarding issue.

The Designated Safeguarding Lead (DSL) is Marjorie Lacassagne (Deputy Head of Primary). Elodie Malard and Hasret Batgi are Deputy DSLs.

The DSL has lead safeguarding oversight of online safety, including understanding the filtering and monitoring systems and processes in place. The IT Manager is responsible for technical implementation and reporting. The Senior Management Team and governing body are responsible for assurance, including reviewing reports, risks, checks and any actions required.

Our staff work closely with the School's DSLs who, in turn, work with the Local Safeguarding Children Partnership (*CSCP - Camden Safeguarding Children Partnership)* and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of CFBL.

CFBL will not tolerate any illegal material and will always report illegal activity to the police and/or CSCP. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-bullying Policy.

Any incident or concern relating to e-safety must be reported to the DSL as soon as possible and recorded on CPOMS in line with the School's safeguarding procedures. Staff should ensure that the CPOMS record is factual, timely and includes relevant details of the concern, the pupil(s) involved, any immediate action taken, and any available evidence, such as screenshots, messages, images or device information. Where there is an immediate risk of harm, staff must speak directly to the DSL or a Deputy DSL without delay, in addition to recording the concern on CPOMS.

4. Staff awareness

Teaching and support staff receive this Policy and the Use of Telephone, Email Systems & Internet Policy and Social Media Policy for staff (in the staff Handbook). All teaching staff receive regular information and training on e-safety issues, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School e-safety procedures. When children use School computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community.

Any incident or concern relating to e-safety must be reported to the DSL as soon as possible and recorded on CPOMS in line with the School's safeguarding procedures. Staff should ensure that the CPOMS record is factual, timely and includes relevant details of the concern, the pupil(s) involved, any immediate action taken, and any available evidence, such as screenshots, messages, images or device information. Where there is an immediate risk of harm, staff must speak directly to the DSL or a Deputy DSL without delay, in addition to recording the concern on CPOMS

5. Online Safety in the curriculum and School community

ICT is a crucial component of every academic subject and is also taught as a subject in its own right in Primary and as part of their Technology class in Secondary.

All of the School's classrooms are equipped with interactive whiteboards, projectors and computers. CFBL has one ICT dedicated room in the School and pupils may use the computers for their Schoolwork in the library

(*CDI*) or the study room (*Salle d'étude)* under a teacher's or a teaching assistant's supervision. There is Wi-Fi connection available for pupils when working in classrooms, under the supervision of teachers, on School laptops or tablets which are monitored in the same way as computer terminals.

IT and online resources are used increasingly across the curriculum. All of CFBL's pupils are taught how to research on the internet and to evaluate sources. They are taught about the importance of evaluating the intellectual integrity of different websites and why some apparently authoritative sites need to be treated with caution.

Pupils will be taught to identify and respond critically to misinformation, disinformation, fake news, conspiracy theories, manipulated media and AI-generated content. They will also be encouraged to seek support from a trusted adult where such content causes concern, promotes harm, or appears to target or exploit children and young people.

We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually seek new opportunities to promote online safety and regularly monitor and assess pupils' understanding of it. We also believe parents are an important part of the e-safety culture and we offer parents regular advice about e-safety on the CFBL newsletter. We also work with the Parents Association to offer free e-safety conferences.

The School provides opportunities to teach online safety within all subjects. Pupils are also educated about the risks associated with technologies they may encounter outside School.

At age-appropriate level, via ICT lessons (but not only), pupils are taught to look after their own online safety. From CE2 (year 4) pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL.

From 5ème (year 8) pupils are also taught about relevant laws applicable to using the internet; such as data protection (including their rights under UK data protection laws) and intellectual property. Pupils are taught to respect other people's information and images (etc.)

The DSL is CFBL's Coordinator for Online Safety, and has particular responsibility for ensuring pupil compliance with the School's e-safety policies and informing all members of the School community about e-safety.

Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see CFBL's Anti-Bullying Policy). Pupils should approach the DSL as well as parents, peers and other School staff for advice or help if they experience problems when using the internet and related technologies.

Vulnerable Pupils: CFBL recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with special educational needs and disabilities (SEND) or mental health needs, and children experiencing trauma or loss. CFBL will ensure that differentiated and ability-appropriate e-safety education, access and support is provided to vulnerable pupils.

6. Use of School and personal devices

School's mobile technologies are only available for pupils to use under the supervision of a teacher or a pupil supervisor.

Pupils are not allowed to use their mobile phones or personal electronic devices in the School, see the School Rules (*Règlement Intérieur*). CFBL pupils are not allowed to connect to the internet with their personal devices inside the School.

For the purposes of this Policy, references to mobile phones and personal electronic devices include smartphones, smartwatches, fitness trackers, tablets, earbuds, or any smart technology capable of messaging, recording, photographing, filming, connecting to the internet, sending notifications or sharing data.

7. Use of internet and email

All pupils are issued with their own School email address for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and can be used for all Schoolwork, assignments /research /projects. CFBL Technology Charter (Appendix 1) and, from 2026/2027, CFBL acceptable use policies (Appendices 2 and 3) set out the agreement between the School and pupils on the use of IT in the School.

There is strong anti-virus, filters and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for Schoolwork / research purposes, pupils should ask their teacher to contact the IT Administrator for assistance.

Pupils should immediately report to a teacher or to another member of staff 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.

In Primary, pupils have to use a specific child friendly search engine (Qwant Junior) which is recommended by the French Ministry of Education.

Pupils must report any accidental access to materials of a violent or sexual nature directly to a teacher or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the School's Behaviour and Discipline Policy.

Pupils should keep their personal, family and social lives separate from their School IT use and limit as far as possible any personal use of their School accounts.

8. Monitoring and access

Parents and pupils should be aware that School email and internet usage (including through School Wi-Fi) will be monitored for safeguarding purposes, and both web history and School email accounts may be accessed by the School where necessary – including serious misconduct or welfare concerns, extremism and the protection of others. Teachers may monitor internet usage in the classroom.

Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The School may require staff to conduct searches of pupils' personal accounts or devices if they were used for School business in contravention of this Policy.

We implement rigorous filtering to limit students' exposure to risks via the School's IT systems by blocking harmful and inappropriate content. Our governing body ensures that our School has effective, age-appropriate filtering in place, and conducts regular reviews to assess their effectiveness.

CFBL will carry out and document at least annually a review of its filtering and monitoring systems, including checks that filtering and monitoring are working effectively on all relevant School-managed and internet-connected devices and in all relevant locations. The review will involve the DSL, IT staff, senior leaders and the responsible governor/trustee, and actions arising will be recorded and followed up.

(*Age-appropriate filtering is already enabled across Google and YouTube services. Regarding web filtering, the system does not currently allow filtering rules to be differentiated by age group. However, all harmful and inappropriate content categories are blocked in accordance with our safeguarding and online safety requirements.*)

CFBL recognises that generative artificial intelligence can create or amplify safeguarding risks, including harmful or inappropriate content, deepfakes, impersonation, misinformation, grooming, bullying, sexualised image

generation, academic misuse, fake intimacy and harmful advice. Any use of AI tools in School must be authorised, age-appropriate, risk-assessed and subject to appropriate filtering, monitoring, data protection and safeguarding controls, following UK and French guidance.

CFBL recognises cyber security as part of safeguarding. The School will maintain appropriate security controls to protect pupil, family, staff and safeguarding information, and will review cyber-security risks, including phishing, malware, ransomware, unauthorised access, compromised accounts and data breaches. Cyber incidents involving pupil welfare or safeguarding information will be reported to the DSL and managed in line with safeguarding and data-protection procedures.

9. Password security

Pupils have individual School network logins, email addresses and storage folders on the server. They are regularly reminded to change their passwords, and of the need for password security. Pupils understand that logging in under someone else's account is identity theft and is prohibited and sanctioned.

All pupils should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every 3 months;
- not write passwords down; and
- should not share passwords with other pupils or staff.

10. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for ID theft, deepfakes, cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

Please refer to the School's Taking, Storing and Using Images of Children Policy for further details including when the School will seek the consent of parents and/or pupils on the use of pupil's images.

For Early years:

- parents are generally prohibited from taking any photographs of children in the early years setting, except for special events such as School performances where they may do so on the understanding that the images are not posted onto social media sites or otherwise shared;
- staff seek parental permission to take photographs of the children, which must be linked to teaching the curriculum and that they use School equipment only for this purpose;
- staff may use personal mobile phones including all electronic devices with imaging and sharing capabilities only during breaks without the presence of the pupils.

11. **Sanctions in case of breach of this Policy**

Please refer to the School's Behaviour and Discipline Policy for sanctions applicable in case of breach of this Policy.

School's reputation: When posting and communicating online or social media, CFBL pupils are expected to have regard for and be mindful of the possible consequences on the School's reputation of their posts and messages. Posts or messages actually or potentially damaging to the School's reputation could result in disciplinary and/or legal action.

12. **Complaints**

As with all issues of safety at CFBL, if a pupil or a parent has a complaint or concern relating to e-safety, prompt action will be taken to deal with it. Complaints should be addressed to the DSL (currently Ms Marjorie Lacassagne) in the first instance, who will undertake an immediate investigation and liaise with the senior management team and any members of staff or pupils involved. For further information, please refer to the Complaints Policy (for parents) and Grievance Procedures (for staff).

_____

Last review by management: June 2026.

Related policies:

- Child Protection & Safeguarding Policy
- School Rules (Règlements intérieurs)
- CFBL Technology Charter (Appendix 1)
- Acceptable Use Policy for Primary School Pupils from 2026/2027 (Appendix 2)
- Acceptable Use Policy for Secondary School Pupils from 2026/2027 (Appendix 3)

Audit trail

Previous policy: 24.03.25

Current 26.06.26

Document Owner and Approval

The Designated Safeguarding Lead is the owner of this document and is responsible for ensuring that it is reviewed in line with the School's policy review schedule.

Appendix 1 - CFBL Technology Charter 2026/2027

Rules pertaining to the use of technology, devices and the Internet

All students who use School computers, devices, systems or online services, including in the CDI, classrooms, Vie Scolaire or any other School area, must follow the School's rules for the use of technology. Students must use all software, hardware, School accounts, networks and online resources responsibly, safely and in accordance with School rules and applicable law.

Technology resources are provided for educational purposes, including classwork, homework, research and other learning activities authorised by the School.

Respect for equipment and the School network

Students must respect the equipment made available to them and must not interfere with the proper functioning of the School network or systems.

Students undertake:

● to take reasonable care of all School equipment
● to follow the instructions given by teachers and staff when using computers, tablets, Chromebooks, iPads, laptops or any other device
● not to damage, misuse, alter or interfere with School equipment, software, settings, accounts, networks or systems
● not to carry out activities that may overload, disrupt or compromise the School network or prevent others from using it properly
● to report any technical problem, error, damage, suspicious activity or security concern to a teacher or member of staff

Access to computing resources

The School provides students with access to a range of computing resources, which may include a School email address, username, password, personal storage space and access to online learning platforms. Students are supported and guided in their use of computers, the internet, digital networks and online resources.

Each student is given an individual account, with a username and password, to access the School's educational network and digital resources.

Students undertake:

● to use School computing resources only for educational activities, Schoolwork, homework or authorised research
● to use only their own login and password
● not to use another person's login, password, account, files or storage area
● not to share their password with anyone else
● to keep their password safe and secure
● to log out of School accounts and devices when they have finished using them
● to ask a teacher or member of staff before accessing normally restricted activities, such as chat rooms, online forums, games, gaming websites, downloads, software installation or file-sharing services
● not to bring files into School, download files, open attachments or connect external storage devices unless this has been authorised by a teacher or member of staff

If a student forgets or loses their password, they should ask Vie Scolaire for help. Password resets may take up to 24 hours to take effect.

Privacy, personal information and files

Everyone has the right to privacy and to the protection of their personal information, image, work and files. Students must respect their own privacy and the privacy of others.

Students undertake:

● not to access, copy, change, delete, move or share information, files or work belonging to another student, member of staff or the School without permission
● not to give out personal information online, including home address, phone number, personal email address, photographs, videos, School details or information about family or friends, unless a teacher has given permission
● not to publish, upload, send or share photos, videos or recordings of another person without their permission and the permission of a teacher where required
● to tell a teacher, the DSL or another trusted adult if they see or receive something online that is worrying, upsetting, fake, harmful, inappropriate or unsafe

Intellectual property and responsible use of information

Students have rights over work they create themselves. They must also respect the intellectual property rights of others, both online and offline.

Students undertake:

● to respect the work, images, music, writing, videos, ideas and creations of others
● not to copy, reproduce, publish or share another person's work without permission
● not to use illegal, pirated, copied or unauthorised software
● to use online information honestly and responsibly, including acknowledging sources where required
● to understand that Schoolwork may be checked for inappropriate copying, plagiarism or misuse of digital tools

Email, messaging and online communication

Private electronic correspondence is protected by privacy rules, but this privacy is not absolute. If an email, message or online communication raises a concern, causes harm, breaks School rules or presents a safeguarding concern, the School may investigate and take appropriate action.

Students are informed that School email and internet use, including use through the School Wi-Fi, may be monitored for safeguarding purposes and to implement School rules. Web history and School email accounts may be accessed by the School where necessary and proportionate. Teachers may also monitor internet use in the classroom.

Students undertake:

● to use School email and online communication tools responsibly and respectfully
● to send messages that are polite, sensible and appropriate
● not to send anonymous, bullying, threatening, discriminatory, abusive, sexualised, humiliating or harmful messages
● not to forward chain letters, harmful content or inappropriate material
● not to harass, intimidate, threaten, impersonate or harm another person online
● to report any message or online contact that makes them feel uncomfortable, unsafe, worried or upset

Use of AI and digital tools

The School recognises that artificial intelligence and other digital tools can support learning when used appropriately. Students may only use AI tools, image-editing tools or other online services when authorised by a teacher and in line with School guidance.

Students undertake:

● to use AI and digital tools only when permitted by a teacher and for the purpose set by the School
● to use AI tools honestly, safely and responsibly
● not to use AI tools, image-editing tools or online services to create, alter or share fake, misleading, intimate, humiliating, discriminatory, abusive or harmful images, videos, audio, messages or documents
● not to use technology, apps or AI tools to pretend to be someone else, impersonate another person, create fake accounts, trick others or damage someone's reputation
● to report any concerning AI-generated content, deepfake, impersonation, harmful image or online interaction to a teacher, the DSL or another trusted adult

PCs, iPads, Chromebooks and other School devices

The School may allow students to use PCs, iPads, laptops, Chromebooks and other School devices for learning activities.

Students undertake:

● not to take photos, videos or sound recordings on any device without the express permission of a teacher
● not to change device settings, including desktop images, notification sounds, Bluetooth, Wi-Fi, network settings or accessibility settings, unless instructed by a teacher
● not to send, share or broadcast images, videos, audio or files using Bluetooth, Apple TV, AirDrop, email, messaging apps or any other method without the express permission of a teacher
● not to activate airplane mode or change Wi-Fi or Bluetooth settings
● not to use Bluetooth headsets, earbuds, headphones, a mouse or any other external device unless authorised by a member of staff
● to sign out of their accounts before returning or leaving a School device
● to understand that damage, vandalism or deliberate misuse of devices may lead to sanctions and parents may be asked to contribute to the cost of repair or replacement

Wi-Fi, mobile networks and internet access

Students may only use the School's Wi-Fi network with permission from a teacher or member of staff. The use of mobile internet networks, including 3G, 4G or 5G, is not permitted on School premises.

Any unauthorised use of the School Wi-Fi, mobile networks or other internet access may lead to confiscation of the device and sanctions in line with the School's Behaviour & Discipline Policy.

Keeping the School network safe

The School uses filtering, monitoring and security systems to help protect students and the School community. Certain websites and services may be blocked by the School's filtering system or IT staff.

To protect the School network, access to USB flash drives and other removable devices is restricted. Any pupil or member of staff who wishes to connect a removable device to the School network must arrange this in advance with the IT Manager so that it can be checked for viruses, security risks and compliance with the School's data-protection and security requirements.

Students undertake:

● not to try to bypass filtering, monitoring or security systems
● not to use VPNs, proxy sites or other tools to access blocked content
● not to introduce viruses, malware or harmful files onto the School network
● to report suspicious emails, links, pop-ups, files, scams or requests for personal information to a teacher or member of staff

Mobile phones and personal devices

The use of mobile phones, smartphones, smartwatches, Apple Watches, Fitbits, fitness trackers, earbuds, tablets, cameras, recording devices and all other personal electronic or smart devices is strictly forbidden at all times on the School premises, unless specifically authorised by the School.

On arrival at School, these devices must be switched off and stored securely in phone pouches. They must not be used in any way during the School day. Pouches will be open at the end of the day when the students are leaving the premises and phones must not be switched on until the student has left the School premises. No student may keep a mobile phone or personal device on their person during the School day.

Staff may confiscate any personal electronic device that is seen or heard during the School day or suspected of being used in breach of School rules. Sanctions may be imposed on pupils who use personal electronic devices in School.

Respect, safety and British law

Students must respect the rights, dignity, privacy and safety of others when using technology. This applies to School devices, personal devices, School accounts, email, social media, messaging, online gaming, websites and any other online platform.

Students undertake:

● not to harass, bully, threaten, humiliate or harm another person online
● not to send, publish, upload or share anything abusive, defamatory, discriminatory, sexualised, violent, extremist, illegal or otherwise inappropriate
● not to access, create, store, send or share illegal or harmful material
● not to publish, upload or send photos, videos or recordings of another person without permission
● not to engage in online behaviour that could harm another person, the School community or the reputation of the School
● to seek help from a teacher, the DSL, a Deputy DSL or another trusted adult if they are worried about something they have seen, received, done or been asked to do online
● to keep asking for help until someone listens

Students must understand that misuse of technology may lead to sanctions under the School's Behaviour and Discipline Policy and may also be referred to the DSL, parents, external agencies or the police where appropriate.

Appendix 2 - Acceptable Use Policy for Primary School Pupils from 2026/2027

Name:
School:
Class:

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

Use School technology safely
● only use the internet when my teacher says it is okay
● only open pages which my teacher has said are okay
● only use my School email address
● only email people I know or if my teacher agrees
● talk to my teacher before using anything new on the internet

Keep my information private
● keep my password secret
● not use other people's login or password
● not tell people personal information about myself online, such as my name, where I live or where I go to School
● not give personal data, such as my mobile number, home number or address, to anyone online

Be kind and respectful online
● make sure all the messages I send are polite
● not reply to any nasty message which makes me feel upset, uncomfortable or unsafe
● not use technology, apps or AI tools to pretend to be someone else, make fake pictures or videos, or upset, trick or embarrass another person

Stay safe with images, videos and people online
● not upload photographs of myself onto the computer or online
● tell a trusted adult if I see a fake, worrying or upsetting image, video or message online
● never agree to meet a stranger or someone I have only met online

Ask for help
● tell my teacher, the DSL or another trusted adult straight away if something online worries me, scares me, upsets me, or makes me feel uncomfortable or unsafe
● tell my teacher if I get a nasty message
● keep asking for help until someone listens

Parents
□ I have read the above School rules for responsible internet use and agree that my child may have access to the internet at School. I understand that the School takes reasonable and proportionate steps, including filtering and monitoring, to reduce the risk of pupils accessing harmful or inappropriate online content. I also understand that no filtering or monitoring system can remove all risk, and that the School will respond to any concern in line with its safeguarding, behaviour and online-safety procedures.
□ I understand that my child's work may be published or shared by the School only in accordance with the School's privacy notices, image-use consent arrangements and Taking, Storing and Using Images of Children Policy.

Signed:
Date:

Appendix 3 - Acceptable Use Policy for Secondary School Pupils from 2026/2027

Name:

School:

Class:

I understand that all computer equipment is owned by the School and that I can use the internet at School as long as I behave in a responsible way that keeps me and others safe. I also understand that the School ICT system is monitored and that if I do not follow the rules, I may not be allowed to use the School computers.

I will:

Use School technology responsibly
● only use the School's computers for School work and homework
● ask a member of staff for permission before using the internet
● not visit websites I know are banned by the School
● not use non-School email accounts or social networking sites in School
● not bring files into School without permission
● not open attachments or download files unless I have permission or I know and trust the person who sent them
● log out when I have finished using the computer

Protect accounts, files and personal information
● keep my login and password safe
● not let anyone else use my login or password
● not use anyone else's login or password
● only delete my own files
● not look at other people's files without their permission
● not give out my home address, phone numbers, photographs, videos or any other personal information that may identify me, my family or my friends, unless my teacher has given permission

Communicate respectfully online
● only email people I know or whom my teacher has approved
● make sure any messages I send or information I upload is polite and sensible
● not use any internet system to send anonymous or bullying messages
● not forward chain letters
● not impersonate another person online or use fake accounts to mislead, bully, harass or harm others

Use AI and digital tools safely
● not use AI tools, image-editing tools or any online service to create, alter or share fake, misleading, intimate, humiliating or harmful images, videos, audio or messages
● report any concerning AI-generated content, deepfake, impersonation, harmful image or online interaction to a trusted adult or the DSL

Stay safe online and with devices
● never arrange to meet someone I have only met online unless my parent, carer or teacher has given me permission and I will take a responsible adult with me
● not use my mobile phone or other personal device in School

Ask for help and report concerns
● tell my teacher or a responsible adult if I see anything I am unhappy with or receive a message I do not like
● not respond to bullying messages
● report online safety concerns, including bullying, harassment, grooming, sexualised content, image-sharing, impersonation, scams or threats, to a teacher, trusted adult, the DSL or Deputy DSL
● seek help even if I am worried that I have made a mistake or broken a rule

Signed:

Date:

Parents

□ I have read the above School rules for responsible internet use and agree that my child may have access to the internet at School. I understand that the School takes reasonable and proportionate steps, including filtering and monitoring, to reduce the risk of pupils accessing harmful or inappropriate online content. I also understand that no filtering or monitoring system can remove all risk, and that the School will respond to any concern in line with its safeguarding, behaviour and online-safety procedures.

□ I understand that my child's work may be published or shared by the School only in accordance with the School's privacy notices, image-use consent arrangements and Taking, Storing and Using Images of Children Policy.

Signed:

Date: