Collège Français Bilingue de Londres

("CFBL" or the "School" or “we”)

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

Authorised by:	The Board of Governors of CFBL
Last review:	WR 22 November 2023
Review Date:	A least annually November 2024 or sooner following any updates to national and local guidance and procedures
Circulation:	Governors/all staff/volunteers, automatically; Staff: Shared drive > Policies Parents: on request/School Website

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 E-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.*

E-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

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 IT and internet and Social Media Policy (for staff) ;
- Staff Behaviour Policy;
- *Charte informatique* (for pupils);
- General Privacy Notice (for all school community);
- Privacy Notice (for pupils aged 13 +);
- Privacy Notice (for staff);
- PSHCE;
- 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, the *Charte Informatique* (for pupils) and the Use of IT and Internet and 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 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.

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 the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board. 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 inform parents of e-safety issues.

<u>Role of our Designated Safeguarding Leads (DSLs)</u>

The School recognises that internet safety is a child protection and general safeguarding issue.

The DSL for the primary is Marjorie Lacassagne (Deputy Head of Primary) and the DSL for the secondary is Jean

Saillard (Deputy Head of Secondary). Elodie Malard and Vincent Wiemann are Deputy DSLs.

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.

A record of concern (Appendix 3, also available of the Staff Shared Drive > Policies > Report forms) must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the School's DSL for the primary or DSL for the secondary (as appropriate).

Staff awareness

Teaching and support staff receive this Policy and the 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.

Incidents of or concerns around e-safety will be recorded using a Record of Concern form (See Appendix 3) or an Incident Report form and reported to the DSL in accordance with the School's Child Protection Policy. Both forms are available on the Staff Shared Drive > Policies > Report forms.

E-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 educated into the importance of evaluating the intellectual integrity of different websites and why some apparently authoritative sites need to be treated with caution.

We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our 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 Association of Parents to offer free e-safety conferences.

The School provides opportunities to teach about e-safety within all subjects. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out in all subjects.

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 DSLs for the primary or secondary.

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 about respecting other people's information and images (etc.)

The Deputy Head Teacher for Secondary, Jean Saillard, is CFBL's Coordinator for Online Safety, and has particular responsibility for ensuring pupils' 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 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.

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 pupils' 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.

Use of internet and email

All pupils are issued with their own personal School email addresses 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 (see Appendix 1) sets 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 accounts.

Appendix 2 sets out the rule applicable in case remote teaching is being used by the School at any time.

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.

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.

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 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 ask the consents 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, but for special events such as school performances, 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 use personal mobile phones only during breaks without the presence of the pupils.

Sanctions for misuse of school IT

Please refer to the School's Behaviour and Discipline policy for sanctions applicable in case of violation of this E-safety and Use of Internet, Mobile Phone and Other Electronic Equipment Policy for Pupils.

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 in charge of Online Safety (currently Jean Saillard) 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 and safeguarding trustees: November2023.

Appendix 1 - CFBL Technology Charter

CFBL TECHNOLOGY CHARTER 2023/2024

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

All students who make use of school computers and systems (in the CDI, in classrooms, in Vie Scolaire etc.) must follow and accept the internal terms of use of both software and hardware as defined by the school and all rules and regulations as defined in British Law.

This form is automatically collecting emails from all respondents. Change settings

Respect the rules of computer ethics

IT resources are made available to all students for the sole purposes of partaking in educational activities or conducting research for academic purposes.

Everyone must respect the equipment made available and must not interfere with the proper use of the network. Students undertake:
- To take all reasonable care of the equipment
- To respect the rules of use of computer equipment as specified by the teachers
- Not to perform activities which may hog computer resources and penalize the community

Each and every student's personal information and files will be protected. Students undertake:
- To respect all health & safety regulations
- Not to introduce, modify, alter, delete or copy information not belonging to themselves
- Not to access any information belonging to the school or any other user without authorisation
- To inform a teacher of any anomaly they may see anywhere on the system

Access to computing resources

The school offers all students enrolled in the school a variety of computing resources (email address, username and personal login password, personal data storage facilities, online homework access). Students are supported, advised and guided in their use of computers, use of the Internet and digital networks and resources. Each student is assigned an individual account (username and password) that allows them to connect to the school's educational network and access full computer-based resources.

Students undertake:
- Not to disclose their password to any other users; each student is responsible for the use of computers through their own user code.
- Not to use any user code apart from their own to access a school computer.

Each student may access the school's computing resources to partake in educational activities or to conduct research for academic purposes. Students will need to obtain permission from a teacher or another responsible person before engaging in any normally forbidden activity such as the use of chat rooms and online forums, downloading software or documents of any kind or playing games or accessing game websites.

Each student must keep their password safe and secure. In the event a student loses his password, they will no longer be able to access their accounts and may not be able to participate in normal class activities. They may request their password be reset by asking Vie Scolaire, however, this may take up to 24 hours to take effect

Intellectual property & privacy of correspondence

Each student has the intellectual property ownership rights over each and every work created by themselves. Their permission will always be required prior to reproducing, copying, cloning etc. be it sound, image, text etc. All students will be asked for their permission prior to any reproduction or republishing of their works.

Students undertake:
- To respect the intellectual property rights of others, both online and offline
- Not to make copies of software not authorized by law
- Not to use illegal, pirated or copied software
- Not to publish reproductions without previously obtaining the permission of their creator(s).

Private electronic correspondence enjoys protection: the privacy of correspondence. This means that when writing a private email or other form of correspondence, students may have an expectation of privacy. However, this is not absolute: for example a student, their parents or someone else may complain that an email is inappropriate or causes concern. The school will have a legitimate interest to investigate.
Students are informed that school email and internet usage (including through school Wi-Fi) may be monitored for safeguarding purposes, and both web history and School email accounts may be accessed by the School where necessary for safeguarding purposes or to implement the school rules. Teachers may monitor internet usage in the classroom.

PCs, iPads and Chromebooks

The school will allow the student access to PCs, iPads, laptops and Chromebooks under the following conditions:
1. No photos, films or sound recordings will be made on any device without the express permission of a teacher.
2. Students will not modify any settings including desktop images, notification sounds, Bluetooth or other wireless and network settings.
3. Students will not send, share or broadcast images, films, audio or any other files via Bluetooth, apple tv or other means with other members of the class without the express permission of a teacher.
4. Vandalism or other wanton destruction of the devices will be sanctioned accordingly. Parents will be asked to pay for the cost of a replacement item.
5. Airplane mode will not be activated, nor will any Wi-Fi or Bluetooth setting be touched or modified. Bluetooth headsets or earbuds may not be used.
6. Students must ensure that they are signed out of their accounts before handing in their devices at the end of their lessons.
7. Students will not connect any external device (headphones, mouse, etc.) without the express permission of an adult.

WiFi and Networks

The use of the school's Wi-Fi network is strictly prohibited without having received permission in advance from a teacher or other member of staff. Similarly, the use of mobile internet networks using 3G/4G/5G is strictly prohibited. Any use of such networks will lead to the immediate confiscation of the device in question and may lead to sanction.

Keeping the school network safe

The School adheres to best practice regarding e-teaching and the internet, and to this effect, certain sites are blocked by the School's filtering system and the School's IT Administrator. To the same effect, the school protects its network by restricting access to student's USB flash drives and such like. Any member of staff or pupil who wishes to connect a removable device to the School's network is asked to arrange in advance with the IT Administrator to check it for viruses and to ensure compliance with the School's data encryption policy.

Mobile phones & personal devices

The use of mobile phones, smartphones, iPods, smartwatches, apple Watches, fitbits or other fitness trackers and all other such personal electronic devices is strictly forbidden at all times within the school's premises. Upon your arrival at school, these devices must be switched off and stored securely in either your lockers or your bags. They may not be used in any manner until the end of the school day. Phones may not be switched on until you have left the school premises. No student may have a mobile phone upon their person at any time during the school day. Staff may confiscate any personal electronic equipment that they see being used during the school day. Sanctions may be imposed on pupils who use their electronic equipment at any time in the school.

Respect of British Law & personal privacy

Everyone has a right of respect of their private life (their home life, their image, their creations). They too must, at all times, respect the privacy of their colleagues and the rules of public order. Each student has the right to assume and require that their privacy is respected.

Students undertake in the course of an exchange of emails, social media or web publications etc.:
- Not to harass or harm the dignity of another user including through the use of messages, texts or provocative pictures
- Not to broadcast or publish anything of an abusive or defamatory nature that may prejudice the privacy, rights or the image of others
- Not to publish, upload or send photos on any media without the express permission of the persons depicted.

Students must maintain public order and undertake not to:
- Disseminate information advocating any inappropriate or illegal material.
- Visit any immoral, inappropriate or illegal websites.

Appendix 2 - Charte sur l'enseignement à distance

En cas de mise en place d'un enseignement à distance et afin de poursuivre notre scolarité dans les meilleures conditions voilà les règles de bonne conduite à adopter:

◆ **Sur Pronote:**

- Je consulte mon emploi du temps

- Je prends connaissance des devoirs à faire

- J'organise ma journée de travail, entre les sessions "vidéo live" sur Zoom, les activités données par mes professeurs sur les heures "habituelles", et éventuellement les ateliers proposés par la Vie Scolaire.

Pour votre information, les professeurs continuent à utiliser Pronote pour indiquer les mérites et encouragements, mais aussi les travaux non faits ou les attitudes incorrectes. Vos parents en sont donc automatiquement informés, et la Vie Scolaire continue à en faire le bilan de manière régulière.

◆ **Pendant les sessions "vidéo live" sur Zoom ou Google Meet**

- Je ne partage pas le lien pour permettre l'accès à ma session avec des élèves extérieurs à mon groupe/ ma classe

- Je m'installe dans un endroit calme, neutre, et propice au travail

- J'adopte une tenue et une attitude de travail correctes

- Je ne cache pas mon identité (pseudonyme interdit) ni mon visage (masque, avatar, etc… sont strictement interdits)

- Je n'utilise pas d'arrière-plan virtuel

- Je respecte les règles de participation données par le professeur (prise de parole, chat, partage d'écran, utilisation du tableau)

- Je ne réalise pas d'enregistrement vidéo ou photographique de la session en ligne

◆ **Sur Google Classroom:**

- Je ne rédige pas de commentaires inappropriés

- Je respecte les délais et les conditions données par le professeur pour faire le travail demandé

◆ **Lorsque je communique en utilisant Gmail ou tout autre moyen de communication:**

- J'utilise un langage respectueux et je respecte les formules de politesse, en particulier quand je m'adresse à un adulte

- Je respecte la charte informatique signée en début d'année scolaire et mentionnée dans le Règlement intérieur

Les règles en vigueur au CFBL, en particulier celles indiquées dans la Charte informatique, continueront à être appliquées, et donc l'échelle des punitions et des sanctions peuvent être appliquées si cela est nécessaire.

En cas de non-respect de ces règles d'utilisation, les mesures suivantes seront prises:

- Rappel des règles à l'oral et/ou à l'écrit par votre professeur
- Remarque inscrite sur Pronote et donc communiquée à vos parents
- Courrier à vos parents
- Exclusion temporaire, partiel ou total, du dispositif d'école à distance
- Rendez-vous avec vous, vos parents et la Direction

Appendix 3 - ONLINE SAFETY INCIDENT REPORT FORM

(this form is available on the Staff shared drive > Policies > Report forms)

Details of incident

Date happened:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?

- In school
- Outside school

Who was involved in the incident?

- child/young person
- staff member
- other (please specify)

Type of incident:

- bullying or harassment (online bullying)
- deliberately bypassing security or access
- hacking or virus propagation
- racist, sexist, homophobic, transphobic, bi-phobic, religious hate material
- terrorist material
- online grooming
- online radicalisation
- child abuse images
- on-line gambling
- softcore pornographic material
- illegal hard core pornographic material
- other (please specify)

Description of incident

Nature of incident:

- **Deliberate access**

Did the incident involve material being:

- created
- viewed
- printed
- shown to others
- transmitted to others
- distributed

Could the incident be considered as

- harassment
- grooming

- online bullying
- breach of Acceptable Use Policies
- accidental access

Did the incident involve material being

- created
- viewed
- printed
- show to others
- transmitted to others
- distributed

Action taken

By staff

- incident reported to head teacher / senior manager
- advice sought from LADO (DSLs)
- referral made to LADO (DSLs)
- incident reported to police (DSLs)
- incident reported to Internet Watch Foundation (DSLs)
- incident reported to IT
- disciplinary action be taken (Headteacher)
- online safety policy to be reviewed/amended (Headteacher and Deputy Head Teacher)

Please detail any specific action taken (ie : removal of equipment)

By child/young person

- incident reported to headteacher or DSLs
- advice sought from Children's Safeguarding and Social Work
- referral made to Children's Safeguarding and Social Work
- incident reported to police
- incident reported to social networking site
- incident reported to IT
- child's parents informed
- disciplinary action to be taken
- child/young person debriefed
- online safety policy to be reviewed/amended

Outcome of incident/investigations