Collège Français Bilingue de Londres

("CFBL" or the "School")

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

Authorised by:	The Board of Governors of CFBL
Date:	WR 29 October 2021
Review Date:	A least annually September 2022 and/or 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 existing communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of the School's role to teach pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

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. Our pupils are therefore taught how 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;
- Email and instant messaging;
- Google Classroom;
- Social networking sites;
- Music / video downloads;
- Video calls and classes;
- Podcasting;
- Mobile internet devices such as tablets and Chromebooks
- Zoom

This policy is implemented to protect the interests and safety 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)

- *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 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 Cecile Denais (Deputy Head of Secondary). Elodie Malard and Marie-Anaïs Le Petit are Deputy DSLs.

Our staff work closely with the School's DSLs who, in turn, work with the Local Safeguarding Children Board (LSCB) 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 the LSCB. 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 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 or an Incident Report form and reported to the DSL in accordance with the School's Child Protection Policy.

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 *Salle d'étude* under a teacher's or a teaching assistant's supervision. There is Wi-Fi connection available for pupils when working on School laptops or tablets under the supervision of teachers in classrooms which is 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.

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

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 the GDPR) and intellectual property. Pupils are taught about respecting other people's information and images (etc.)

The Deputy Head Teacher for Secondary, Cécile Denais, 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.

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 *Règlement Intérieur* (School Rules). 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. The pupils' *Charte informatique* 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 <u>must</u> 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 these accounts.

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.

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 their personal accounts or devices if they were used for school business in contravention of this Policy.

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.

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.

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 Cécile Denais) 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 October 2021.

Charte sur l’enseignement à distance

Afin de continuer notre scolarité à distance dans les meilleurs 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

- 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)

◆ 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

CFBL TECHNOLOGY CHARTER 2021/2022

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

All pupils 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.

Respect the rules of computer ethics

IT resources are made available to all pupils. Everyone must respect the equipment made available and must not interfere with the proper use of the network. Each pupil may access the school's computing resources to partake in educational activities or to conduct research for academic purposes. Pupils will:

- Take all reasonable care of the equipment
- Respect the rules of use of computer equipment as specified by the teachers
- Not to perform activities hogging computer resources and penalizing the community

Each and every pupil's personal information and files will be protected. Pupils will:

- Respect all health & safety regulations
- Not introduce, modify, alter, delete or copy information not belonging to themselves
- Not access any information belonging to the school or any other user without authorisation
- Inform a teacher or the of any anomaly they may see anywhere on the system

Access to computing resources

The school offers all pupils enrolled in the school a variety of computing resources (an email address, a username and a personal login password, personal data storage facilities, online homework access). Pupils are supported, advised and guided in their use of computers, use of the Internet and digital networks and resources. Each pupil 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. Pupils undertake: -

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

Each pupil may access the school's computing resources to partake in educational activities or to conduct research for academic purposes. Pupils 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.
You must keep your password safe and secure. In the event a pupil 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

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

Pupils agree to:

- Respect all intellectual property both online and offline
- Not to make copies of software not authorised by law
- Not to use illegal, pirated or copied software
- Not to publish reproductions without previously obtaining the permission of their creator(s).

All private electronic correspondence enjoys protection: the privacy of correspondence. The private correspondence of each pupil is confidential. Pupils will respect the confidentiality and privacy of their colleagues' email and other forms of correspondence under all circumstances.

iPads and Chromebooks

The school will allow the pupil access to iPads, laptops and Chromebooks under the following conditions:

1. No photos, films or sound recordings will be made on the device without the express permission of a teacher.
2. Pupils will not modify any settings including desktop images, notification sounds, Bluetooth or other wireless and network settings.
3. Pupils 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 may be asked to pay for the cost of a replacement item.
5. Airplane mode will not be activated, nor will any WiFi or Bluetooth setting be touched or modified. Bluetooth headsets or earbuds may not be used.
6. Pupils must ensure that they are signed out of their accounts before handing in their devices at the end of their lessons.

WiFi and Networks

The use of the school's WiFi 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.

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 pupil'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 & devices

The use of mobile phones, smartphones, iPods, smartwatches, fitness trackers and 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 your lockers. They may not be retrieved until the end of the school day. Phones may not be switched on until you have left the school premises. No pupil may have a mobile phone upon their person, nor in their bags at any time during the school day. Staff may confiscate 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 pupil has the right to assume and require that their privacy is respected.

Pupils 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.

Pupils must maintain public order and undertake not to:

- Disseminate information advocating any inappropriate or illegal material.

- Visit any immoral, inappropriate or illegal websites.