E-Safety and Use of Internet, Mobile Phones and Other Electronic Equipment Policy

Collège Français Bilingue de Londres
(The "School")

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.

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 and abuse.

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

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

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;
- Social Media Policy (for staff)
- *Charte informatique* (for pupils)
- Data Protection Policy (for pupils and parents)
- Data Protection policy (for staff)
- PSHEC.

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.).

Roles and responsibilities

The Senior Management Team and the IT Systems Administrator have 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 Local Authority, 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 / carers 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 David Gassian (Head of Primary) and the DSL for the secondary is Quentin Dève (CPE). The deputy DSL is Maud Donatucci.

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. All of the School's classrooms are equipped with interactive whiteboards, projectors and computers. CFBL has ICT dedicated rooms in the school and pupils may use the computers in in the library (CDI) for their school work. 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 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 ICT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out in ICT lessons.

At age-appropriate levels, and usually via ICT lessons, 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 Safeguarding Lead for the primary or for the secondary

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

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

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that they log off to prevent unauthorised access.

Staff are permitted to bring in personal devices for their own use.

Personal telephone numbers may not be shared with pupils or parents / carers and staff are not permitted to contact a pupil or parent / carer using a personal telephone number.

Pupils

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

No personal devices belonging to pupils are to be used during lessons at school. Please refer to the *Règlement Intérieur* for the primary and the *Règlement Intérieur* for the secondary (School Rules) regarding the use of mobile phones in the School.

Use of internet and email

Staff

When accessed from personal or the School's devices, whether on or off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position (please refer to Staff Social Media policy)

There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications are monitored.

Staff must immediately report to the Designated Safeguarding Lead for the primary or the secondary 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.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring CFBL into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links or material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends'.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils are issued with their own personal school e-mail 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 school work, assignments / research / projects. Pupils should be aware that email communications are monitored. 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 and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research] purposes, pupils should ask their teacher to contact the IT Administrator for assistance.

Pupils should immediately report to a teacher or or 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.

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 be aware that all internet usage via the school's systems and its wifi network is monitored.

Data storage

The School takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy (for Pupils and Parents) or the Data Protection Policy (for staff) for further details.

Staff are obliged to save all data relating to their work to their school laptop/ PC or to the school's central server / Google Drive Account.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Administrator.

Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff 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, staff, parents / carers 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.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

In accordance with the guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.), nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

By signing CFBL's T&C, parents or carers consent to CFBL and its staff making use of information relating to their child (including photographs, video recordings and sound voices recordings) to enable CFBL to manage relationships between the School and its pupils and parents or to promote the School or publicise the School's activities. Parents who do not wish the school to film or photograph their child or use his or her image must contact the Headteacher.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Complaints

As with all issues of safety at CFBL, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the IT Administrator 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).

This Policy is drafted taking into account 'Keeping children safe in education' DfE guidance and is reviewed annually.

Last review: 10/2016 (this document replaces the policy called Use of ICT Policy)