Collège Français Bilingue de Londres("CFBL" or the "School")

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

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, carer 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;
- Email and instant messaging;
- Google Classroom;
- Social networking sites;
- Music / video downloads;
- Video calls;
- Podcasting;
- Mobile internet devices such as tablets and Chromebooks

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)
- PSHEC.
- 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 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 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 David Gassian (Deputy Head of Primary) and the DSL for the secondary is Rodrigue Barbosa (Deputy Head of Secondary). 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 and Safeguarding 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) or the Salle d'étude, under a teacher's or a teaching assistant's supervision 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 DSLs 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 from 2018, their new rights under the GDPR) and intellectual property. Pupils are taught about respecting other people's information and images (etc.)

The School's ICT teacher, Adam Benjamin, is CFBL's Coordinator for Online Safety, and as well as teaching e-safety, 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).

Use of internet and email

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. 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 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 web browser (Qwant) 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 be aware that all internet usage via the school's systems and its wifi network is monitored.

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 for a lawful purpose – including serious conduct 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 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 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: 05/2018 (this document replaces the policy called Use of ICT Policy)