LYCÉE INTERNATIONAL DE LONDRES WINSTON CHURCHILL

("the School")

Policy #11: Students' Use of ICT and Electronic Devices

Mission

Through a rigorous, bilingual programme and innovative methods, we educate students to become responsible, creative, and principled global citizens. We teach them to think critically and act ethically, to form and express their own opinions and respect those of others, to define their own life goals, and to make sense of and embrace change.

Our values are: Excellence, Creativity, Integrity, Awareness and Community.

In support of these aims and values we are committed to ensuring the following:

Introduction

The role of technology in our students' lives: 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 students 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.

1. Information & Communication Technology (ICT) in the curriculum.

ICT is a crucial component of every academic subject and is also taught as a subject in its own right. Every classroom in the school is equipped with a Projector, an Apple TV and a sound system. The School has two dedicated ICT rooms and students may use these in the presence of a member of the teaching staff for their school work and for coding or tech clubs. iPads issued to students are configured to

automatically connect to the school WiFi network, which is subject to filtering of inappropriate content, apps and services.

All of the Lycée's students 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 even seemingly reliable sites need to be treated with caution.

As stated in our Charte de Vie Scolaire, the use of mobile phones, electronic games, MP3 or similar, is not allowed during classes except with the authorisation of the teacher for pedagogical reasons. Mobile phones must be on vibrate outside the classroom, and turned off when in class. Electronic games are prohibited at School at all times and should not be downloaded on any school-owned device such as iPad, computer etc.

2. Role of our technical staff and faculty members

With the explosion in technology, the School recognises that blocking and barring sites is not sufficient. The Lycée teaches all students to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for all the faculty members and technical staff. The School's IT Administrator has a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School's hardware system, its data integrity and for training the School's teaching and administrative staff in the use of ICT. They will monitor the use of the internet and will report inappropriate usage to the Head of School in writing when there is serious cause for concern. Teachers can monitor students' iPads in their classrooms, and apply restrictions using the app Apple Classroom.

3. Role of our Designated Safeguarding Leaders (DSL)

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

Our faculty and technical staff have been trained in the safety issues involved in the misuse of the internet and other mobile electronic devices. They 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 the Lycée. All of the staff with pastoral responsibilities have also received training in e-safety issues. Secondary students are taught responsible use of the internet and e-safety through the Pix programme, which includes digital skills and competencies, and the Library's common sense media scheme, providing information and resources for families and

teachers. In the Primary section, classroom teachers are responsible for their students' e-safety ("Permis internet").

When children use the school's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems. However, many pupils are able to access the internet using their own data plan. To minimise inappropriate use, as a school we use web filtering tools for the school computers and we also filter for ipads. This allows us to personalise the privacy settings and allied sites access for pupils who may be more vulnerable. We can generate reports for any safeguarding issues which we are alerted to.

4. Misuse: statement of policy

The School 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 student who misuses technology to bully, harass or abuse another student in line with our anti-bullying policy.

5. Involvement with parents, carers and guardians

The School seeks to work closely with parents, carers and guardians in promoting a culture of e-safety. The School will always contact parents, carers and guardians if it has any concerns about students' behaviour in this area and likewise it hopes that parents and carers will feel able to share any concerns with the School. The School recognises that not all parents, carers and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The School, with its Parents Association also arranges panel discussions and presentations for adults related to the expansion of technology in our life and practical steps families can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity. Weekly iPad assistance sessions are held at school by the Director of Academic Research & Innovation to support families. It is called the Genius bar which provides guidance for parents on online safety and pedagogical matters.

6. Charter for the safe use of the internet and electronic devices

E-safety is a whole school responsibility and at the Lycée, parents are required to agree to an iPad user agreement for the safe use of the internet inside the School or when using the School's facilities. The School expects all students and parents to adhere to the Digital Learning Agreement for secondary. Digital copies are given to all families, and the School may impose sanctions for the misuse, or attempted

misuse of the internet, mobile phones and other electronic devices. For primary education, a lighter version of the Digital Learning Agreement is signed by all the students and displayed in the classroom. There are three different versions depending on the year group: Year1/Year2/Year3, Year4, Year5/Year6.

7. Considerate use of electronic equipment

Mobile phones and other personal electronic devices should be switched off during lesson time. Sanctions may be imposed on students who use their electronic equipment without consideration for others.

There are particular rules relating to electronic devices which allow such devices to be seized and examined for relevant data or files which might offend the law or school rules. Section 550Z of the Education Act 1996 provides for the return of such devices to the pupil but also deals with any offending data or files which may be erased from the device if the staff member believes there are good reasons for doing so.

The school understands that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children can, whilst at school or college, sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content.

At the Lycee International de Londres we manage this risk by: Pix certification, a mandatory assessment for digital safety/literacy at the end of 3eme (Year 10) and Terminale (Year 13). This content is delivered from 5eme (Year 8) during lessons across the school. This is managed and monitored by the Director of Academic Research & Innovation, Head of Years, Class Team Leaders and Teachers. “Heure de vie de classes” aso reinforce and help to distribute this content in secondary school as well as the PSHE curriculum and Common sense media resources.

8. Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim who can be targeted at any time or place. The School's Anti-Bullying Policy describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying.

- Proper supervision of students plays an important part in creating a safe ICT environment at school but everyone needs to learn how to stay safe outside the School.
- The Lycée values all of its students equally. It is part of the ethos of the Lycée to promote considerate behaviour and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff. The victim should never think it is their fault, nor should they be afraid to come forward, report it and seek support.

9. Treating other users with respect

- The School expects students to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. All students agree under the “Digital Learning Agreement” to obey certain rules and obligations; in particular they undertake not to harass or cyberbully others, publish photos or name people without the consent of the person concerned. The School expects a degree of formality in communications between staff and students and would not normally expect them to communicate with each other by text or mobile phones. Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The School's Anti-Bullying Policy is published on the School’s website. The School is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All students are encouraged to look after each other and to report any concerns about the misuse of technology or a worrying issue to a member of the pastoral staff.

10. Keeping the school network safe

- Onsite filtering of all computers is provided by Sophos Web Filter/Firewall.
- The School uses Sophos anti-virus protection on all computers.
- Email services and online file storage for each user is provided by Google Workspace, which has multiple inbuilt safety features such as spam blocking, attachment scanning etc.
- Student iPads are managed using Jamf mobile device management software. This enables the school to control the apps and services available on these devices and allows restricting of inappropriate content both on and offsite.
- Student iPads are monitored during lessons by the teacher using Apple Classroom.

- All users are issued with their own personal email address and network login which is controlled by the IT department.
- Primary students can only send and receive emails within the school domain.
- The School keeps regular backups of all user data, with a secure copy stored offsite.
- The use of USB drives are not allowed.
- Students are forbidden from connecting personal electronic devices to the school network.
- Users are trained in the safe use of the school network on a regular basis.
- Technology and procedures are reviewed regularly and updated as necessary.

11. Promoting safe use of technology

Students and adults are encouraged to make use of the excellent online resources that are available from sites such as:

- UK Council for Child Internet Safety (http://www.education.gov.uk/ukccis)
- Childnet International (www.childnet-int.org)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)

The guidance 'Teaching online safety in school' (DfE, 2019) can be downloaded here:https://www.gov.uk/government/publications/teaching-online-safety-in-schools

- Keeping Children Safe in Education. Statutory guidance for schools and colleges. (DfE: September 2021)
- Sexual violence and sexual harassment between children in schools and colleges 2021https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014224/Sexual_violence_and_sexual_harassment_between_children_in_schools_and_colleges.pdf
- How to Reduce Screen fatigue https://docs.google.com/document/d/13hareQVIocwF38e_kvmLFhOvapg1y7T4k5ONcyTO9l0/edit#heading=h.txon7e7qrz72
- When to turn your camera on and off? https://docs.google.com/document/d/1qHgEEgYw7kD7iBI6yA5SFhFa9dVsJkSB37iM4_u4pmc/edit

- Behaviour Chart for Remote Learning https://docs.google.com/document/d/1DE0x4dX96AglXiiuWAn1DEfSW_z_nDkfUurFg19RMml/edit?usp=sharing
- A Guide for education settings and filtering providers https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring

E-safety is discussed during Heure de Vie de Classes, assemblies and can be discussed in School councils. It is part of our PSHE and Library Hours curriculum.

Safe use of personal electronic equipment

- The School's guidance is that students and staff should always think carefully before they post any information online. Content posted should not be inappropriate or offensive, or likely to cause embarrassment to the individual or others.
- The School implements the Digital Citizenship Curriculum from Common Sense Media to teach internet safety to all students, as part of the PHSE curriculum.
- The School offers guidance on the safe use of social networking sites and cyberbullying.
- The lessons provided by teachers (Parcours Pix, heures de vie de classe, PSHE curriculum) include guidance on how students can identify the signs of a cyber-stalker and what they should do if they are worried about being harassed or stalked online.
- The School offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- The School gives guidance on how to keep safe at home by encrypting the home wireless network, not opening unknown attachments and reporting any illegal content.
- Similarly the School covers how a mobile phone filter can be activated and how to block nuisance callers.
- The use of a VPN on the iPads is strictly prohibited. The School will conduct random checks and students having the VPN installed will be severely sanctioned.
- The School maintains ownership of all digital devices and their content. It reserves the right to erase inappropriate contents or non-school related apps from devices loaned to students for academic purposes.

12. Children and online safety away from school

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Online teaching should follow the same principles as set out in the code of conduct and the behaviour Chart for Remote Learning.

Lycee international de Londres will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider if there are virtual lessons, especially where webcams are involved:

- No 1:1s without parental consent, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms specified by senior managers and approved by our IT network manager / provider to communicate with students
- Staff should record the length, time, date and attendance of any sessions held.

13. Supporting children not in school as they are following clinical or public health advice.

Lycee international de Londres is committed to ensuring the safety and wellbeing of all its Children and Young people.

Where the DSL has identified a child to be on the edge of social care support, or who would normally receive pastoral-type support in school, they should ensure that a robust communication plan is in place for that child or young person.

Details of this plan must be recorded on CPOMS, as should a record of contact have been made.

The communication plans can include remote contact, phone contact, door-step visits. Other individualised contact methods should be considered and recorded.

Lycee international de Londres and its DSL will work closely with all stakeholders to maximise the effectiveness of any communication plan.

This plan must be reviewed regularly and where concerns arise, the DSL will consider any referrals as appropriate.

Lycee international de Londres recognises that school is a protective factor for children and young people, and the current circumstances can affect the mental health of students and their parents/carers.

Teachers at Lycee international de Londres need to be aware of this in setting expectations of students' work where they are at home.

Policy created in 2015.

Policy reviewed in:

- March 2023
- November 2022
- December 2021
- March 2018
- August 2016
- February 2016