ÉCOLE Jeannine Manuel
International understanding through a bilingual education

E-SAFETY POLICY

1 INTRODUCTION

The School recognises the educational and social benefits of using the internet for children, including as a source of information and a means of electronic communication. There is no doubt that, as the use of technology is now universal, children need to learn computing skills in order to prepare themselves for the working environment. Nonetheless, the benefits of using the internet should be balanced against the need to safeguard children against the inherent risks from online technology. Furthermore, the School recognises its role in teaching children, jointly with their parents or guardians, how to keep themselves safe whilst online.

2 OBJECTIVES

2.1 To ensure the safety and wellbeing of our students.

2.2 To promote responsible behaviour with regard to online activities.

2.3 To take account of legislative guidance (see reference documents, paragraph 11).

3 IMPLEMENTATION

All members of the school community share responsibility with regards to adopting a safe conduct online. In particular:

3.1 The Head of School is responsible for the implementation of this policy and will work closely with members of the SLT to ensure that it is effective. She will:

- monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school;
- ensure that staff are aware of this guidance and related guidance (e.g., as can be found in the School's Staff Handbook);
- provide / arrange for staff training;
- maintain records of serious e-Safety incidents and coordinate any investigations;
- provide regular updates concerning e-Safety at school to the Board of Governors;

- ensure the School has appropriate filter and monitoring systems in place and regularly review their effectiveness.

3.2 The Bursar will act as E- Safety Co-ordinator and will:

- report to the Head on recorded incidents;
- liaise with school technical staff;
- liaise with the Head on any investigation and action in relation to e-incidents; and
- advise on e-safety policy review and development.

3.3 The school IT Manager will:

- be responsible for the IT infrastructure and that it is not open to misuse or malicious attack;
- ensure that users may only access the networks and devices through an enforced password protection policy;
- keep up to date with e-safety technical information in order to carry out their role;
- ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse, and that appropriate monitoring and filtering systems are in place; and
- implement any agreed monitoring software / systems.

3.4 Teaching and Support Staff will:

- maintain awareness of the School's e-safety policies and practices;
- report any suspected misuse or problem to the Head of School;;
- ensure that all digital communications with pupils / parents / carers / fellow staff are on a professional level and conducted on school systems (staff should refer to the Staff Handbook & IT Code of Conduct for Pupils for further information on this topic);
- ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- monitor the use of digital technologies (including on iPads, computers etc) during school activities and report any potential issues; and

- ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.5 Pupils:

- are responsible for using school digital technology systems in accordance with the School's IT Code of Conduct for Pupils;
- will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to keep mobile devices switched off at all times while on school premises (except in the case of an emergency), as per the School Rules;
- understand that cyber-bullying is a form of bullying and, as such, that it will not be tolerated by the School (please refer to our School Rules & Anti-Bullying Policy for further information); and
- will understand that the e-safety policy will include actions outside of school where related to school activities or members of the school community.

3.6 Parents / Carers:

- will be advised of e-safety policies through regular communications from the School; communications will most commonly be via email, the school website and through talks held throughout the year.
- are encouraged to support the School in the promotion of good e-safety practice: we believe it is important to model for pupils, and help them learn, how to communicate respectfully and safely with, and about, others online ; and
- should follow school guidelines on:
  - digital and video images taken at school events;
  - their children's / pupils' personal devices in school.

3.7 Governors:

- Ensure online safety is a running and interrelated theme in line with our whole-school approach to safeguarding
- Ensure the School has appropriate filter and monitoring systems in place and regularly review their effectiveness
- Ensure the leadership team and relevant staff fully understand the measures in place and know how to escalate concerns when identified

4 E-Safety in the curriculum

Staying safe online is a focus in all areas of the curriculum and we are constantly looking for new ways to promote e-safety for our pupils. We aim to build pupil resilience across the curriculum so that students can manage their online experience safely, protect their digital identity as well as understand how to identify and deal with online risks.

Students learn about e-safety as part of the curricula of RSHE, PSHCE, EMC (Moral and Civic Education), and SNT (Digital Science and Technology). We ensure that the 4Cs of online risk (content, contact, conduct and commerce) are taught explicitly in an age-appropriate way. Topics covered include:

- Different uses of the internet
- Identities and online relationships
- Cyberviolence and cyberbullying (and how to seek help if they become victims and/or how to report if they become bystanders)
- Mis/dis-information and how to recognise fake news
- Privacy and security
- Online addiction and gaming

We have also enrolled all our secondary students in Y10-Y13 onto the PIX programme, a French certification which covers topics such as privacy, cyberbullying, communication and develops their digital skills.

Since Covid-19 pandemic, we are aware that young people are relying even more on technology and with this comes an increased risk of online harm and addiction. We are always looking for engaging ways to deliver online safety messages and regularly invite external organisations like for example SWGfL to our School to hold e-safety workshops for our secondary students.

5 USE OF TECHNOLOGY IN THE CLASSROOM

Pupils have access to shared laptops and iPads at school. Devices are used by teachers to supplement lessons when needed with the sole purpose of enhancing pupils' learning experience. Students in Y12 and Y13 are allowed to bring their own device and connect to the school's student Wi-Fi – "Jmanuel (Students)".

Students have access to email (Gmail), Pronote, search engines, Google Classroom and other Google sites e.g. Google Docs, Sheets, Slides, Calendar etc. They use the internet to aid classroom learning through research, to develop their ICT and research skills, to investigate careers and to send internal emails to their peers and teachers. Pupils also use apps but always under teacher instruction. Examples include Garageband to create music and reading programmes to develop their reading skills. All students are expected behave responsibly online at all times as per the IT Code of Conduct.

Staff are vigilant during use of websites/technology and will monitor for any potential risks.

Parents are encouraged to do the same at home. In any instance where inappropriate content is suspected or observed, staff members will respond accordingly as per the School Rules.

Content used to bully others will be taken very seriously as per the Behaviour and Anti-Bullying Policy.

6 FILTERING SYSTEM

The School is responsible for ensuring its network is as safe and secure as reasonably possible. We use firewall devices and content filtering tools and regularly updated firewall and filtering rules to restrict access to inappropriate sites on our network. The system logs all attempts to access inappropriate content and this is monitored regularly by the IT department. Please refer to our risk assessments for further information.

Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms would contravene its E-safety Policy.

7 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8 Child protection

Those responsible are trained in e-safety issues and aware of the implications that may arise from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate contact on-line with adults / strangers;
- potential or actual incidents of grooming; and
- cyber-bullying.

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the School's DSL who will decide whether or not a referral should be made to Children's Safeguarding and Social Work or the Police.

Note that staff, including in the EYFS, must not use personal phones, cameras, or other devices capable of taking and sharing images when they are teaching or with students. School devices are available for staff who need to take pictures.

9 Data protection

All data collected via the monitoring of pupil's or staff online activity will be handled in accordance with the UK GDPR. Further information can be found in our Data Protection Policy, in the Privacy Notices on the school website, or by contacting dpo@jmanuel.uk.net.

10 Protection from cyber attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure

- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security.

- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents

- Investigate whether IT software needs updating or replacing to be more secure

- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data

- Put controls in place that are:
    - Proportionate: the school will verify this using a third-party audit to objectively test that what it has in place is effective
    - Multi-layered: everyone will be clear on what to look out for to keep our systems safe
    - Up to date: with a system in place to monitor when the school needs to update its software
    - Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be

- Back up critical and store these backups on cloud-based backup systems

- Make sure staff:
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely

- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights

- Have a firewall in place that is switched on

- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification

- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident.

11 Reference Documents

Legal Requirements & Education Standards

- Commentary on the Regulatory Requirements September 2018, Part 3 (www.isi.net)
- UK Council for Child Internet Safety (www.edcuation.gov.uk/ukccis)
- Cyberbullying Research Center (cyberbullying.org)
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 (UK GDPR)
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges
- Teaching online safety in Schools, DfE: June 2019 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf)

Useful Resources for Teaching e-Safety

- NSPCC guidance on online safety for parents (https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/)
- NSPCC guidance on online safety for teachers (https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/)
- Childnet International (https://www.childnet.com/)
- UK Safer Internet Centre (https://www.saferinternet.org.uk/)
- Think U Know (https://www.thinkuknow.co.uk/)