ONLINE SAFETY POLICY

SUMMARY OVERVIEW

This is a summary of The BRIT School's *Online Safety Policy*. The full policy can be found in the Policies section of the school's website www.brit.croydon.sch.uk

TO WHOM DOES THE POLICY APPLY?

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of The BRIT School IT systems, both in and out of the school.

The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety is delegated to the Online Safety Coordinator.

The Online Safety Coordinator Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.

The IT Support Department are responsible for ensuring that the school's IT infrastructure is secure and is not open to misuse or malicious attack; and that The BRIT School meets the online-safety technical requirements outlined in this document.

Teaching and Support Staff are responsible for ensuring that they have an up-to-date awareness of online-safety matters and of the current school online-safety policy and that safe IT practices are embedded into all aspects of the curriculum and other school activities. Staff are also responsible for ensuring that Students understand and follow BRIT School online-safety and acceptable use policy.

The Designated Persons for Child Protection is trained in online-safety issues, and is aware of the potential for serious child protection issues to arise from IT and online use.

Students are responsible for using The BRIT School IT systems in accordance with the Student Acceptable Use Agreement, which they are expected to sign before being given access to IT systems. Students should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. They should also understand the importance of adopting good online-safety practice when using digital technologies out of school, and realise that the Online-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers are responsible for endorsing the Student Acceptable Use Policy and reading all policies relating to their child's use of IT.

ONLINE-SAFETY EDUCATION IS PROVIDED IN THE FOLLOWING WAYS:

Students' education in online-safety is an essential part of the School's online-safety provision. Young people need the help and support of the staff to recognise and avoid online-safety risks and build their resilience

- Key online-safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students are taught to acknowledge the source of any information used and to respect copyright.
- All students must agree to and sign the school's IT Acceptable Use Policy

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents may either underestimate or not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

Teaching & Support Staff receive online-safety training and understand their responsibilities, as outlined in the Online Safety Policy.

- Various modes of training are adopted to ensure staff are trained and kept up-to-date with online safety issues.
- All new staff should receive online-safety training as part of their induction programme, ensuring that they fully understand this policy and Acceptable Use Policies
- This Online-Safety policy and its updates will be presented to and discussed by staff in team meetings.

HANDLING INCIDENTS

The BRIT School will take all reasonable precautions to ensure online safety. Full details on Handling Incident, including those involving 'sexting' can be found in the full Online Safety Policy, in the Policies section of The BRIT School website: www.brit.croydon.sch.uk

- Staff and student are given information about infringements in use and possible sanctions.
- The Designated Safeguarding Lead acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Designated Safeguarding Lead that day.
- Any concern about staff misuse is always referred directly to the Principal, unless the concern is about the Principal, in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

PASSWORD POLICY

All users will have clearly defined access rights to The BRIT School's IT systems. All users will be provided with a username and password by the IT Support Department who will keep an up to date record of users and their usernames.

- The password should be a minimum of 8 characters long (including numbers, letters and characters)
- Only IT support staff will have access to change staff passwords on their behalf
- All users will use unique accounts to support accountability
- Users should never disclose their password to anyone else (including technical staff), or allow another user to use a computer that has been logged in with their user account.

FILTERING

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context.

The current system provides two tiers of defence. The major part of the web filtering is provided by our internet service appliance, followed by a second tier of filtering; all Windows, Mac and Chromebooks on the school network have Computer Management system installed, which allows IT Support and also the classroom teacher to layer on additional white and black listings, and suspend internet access for individual students.

All users have a responsibility to report immediately to the IT Support Department any infringements of the school's filtering policy of which they become aware, or any sites that are accessed, which they believe should have been filtered.

IT & ONLINE ACTIVITY MONITORING

The BRIT school will monitor the activities of users on the school network and on school equipment as indicated in the School Online-Safety Policy and the Acceptable Use agreement. File Services (e.g. Network File shares) and online system (e.g. Office 365, Google Drive) interactions are logged and can be searched using our management tool. All school managed Windows, Mac & Chromebooks have monitoring software installed.. Screen shots and screen recordings are taken of inappropriate usage.

EMAIL SYSTEMS

The BRIT School will:

- Ensure that email accounts are maintained and up-to-date;
- Use a number of technologies to help protect users and systems in the school, including desktop anti-virus, plus and direct email filtering.

The BRIT School provides **staff** with an email account for their professional use. The IT Acceptable Use agreement makes clear that personal email should be through a separate account.

The BRIT School provided **students** with an email account. The IT Acceptable Use agreement makes clear the appropriate use of school email.

MOBILE DEVICES

- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity, and only with expressed permission from the teacher.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.

SOCIAL NETWORKING

Staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

- **Students** are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through online safety tutorial work.
- **Parents** are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.
- **The school** maintains the right monitor use of social networks and to blocks/filter access to social networking sites, unless there is a specific approved educational purpose.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

DIGITAL IMAGES AND VIDEO

The BRIT School will gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school. We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials.

Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students.

Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure, and what to do if they are subject to bullying or abuse.

FURTHER ONLINE SAFETY INFORMATION

Staff
https://www.thinkuknow.co.uk/teachers/
http://www.childnet.com/teachers-and-professionals

Students
https://www.thinkuknow.co.uk/14_plus/
http://www.childnet.com/young-people/secondary

Parents
https://www.thinkuknow.co.uk/parents/
http://www.childnet.com/parents-and-carers

APPENDIX

i. The BRIT School Online Safety Policy;
ii. Staff IT Acceptable Use Policy;
iii. Student IT Acceptable Use Policy;
iv. Data Protection Policy Statement;
v. Privacy Statement;
vi. UKCCIS "Sexting in schools and colleges"
vii. IT Network Filtering Policy