The BRIT School
Online Safety Policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Schedule for Review

This Online Safety policy was approved SLT *on:*	*January 2018*
The implementation of this Online Safety policy will be monitored by the:	*The Safeguarding Officer* *Online Safety Coordinator* *Senior Leadership Team*
Monitoring will take place at regular intervals:	*Annually*
SLT will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*January 2019*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer* *Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of computer and internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of students* / parents/carers / *staff*

Contents

Scope of the Policy

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 Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school

Principal and SLT

- 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 will be delegated to the Online Safety Coordinator
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Principal / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those who carry out the internal online safety-monitoring role. This is to provide a safety net, and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

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 Online Safety Coordinator will:

- Ensure that all staff are aware of the procedures that need to be followed in the event of an online incident taking place;
- Provide training and advice for staff;
- Liaise with IT Support Services;
- Receive reports of online safety incidents and ensures a log of incidents to inform online-safety is kept by the IT Support Team;
- Report regularly to, and liaises with SLT in charge of Child Protection.

IT Support Department

IT Support are responsible for ensuring:

- That the school's IT infrastructure is secure and is not open to misuse or malicious attack;
- That The BRIT School meets the online-safety technical requirements outlined in this document;
- That users may only access the school's networks through a properly enforced password protection policy;
- That the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single-person;
- That they keep up-to-date with online-safety technical information in order to effectively carry out their online-safety role and to inform and update others as relevant;
- That the use of the network / web portals / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online-Safety Co-ordinator for investigation / action / sanction;
- That monitoring software / systems are implemented and updated as agreed.

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 practices;
- They have read, understood and signed the school Staff Acceptable Use Agreement (*See Appendix. a*);
- They report any suspected misuse or problem to the Online-Safety Coordinator / Safeguarding Officer / Principal / SLT;
- Digital communications with students should be on a professional level and only carried out using official BRIT School systems;
- Online-safety issues are embedded in all aspects of the curriculum and other BRIT School activities;
- Students understand and follow BRIT School online-safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor IT activity in lessons, extracurricular and extended school activities;
- They are aware of online-safety issues related to the use of mobile devices and that they monitor their use and implement current BRIT School policies with regard to these devices;
- In lessons, where internet use is pre-planned, students should be guided to sites checked as suitable for their use.

Designated Person(s) for Safeguarding (DSL)

Is trained in online-safety issues and is aware of the potential for serious child protection issues to arise from:

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

Students:

- Are responsible for using The BRIT School IT systems in accordance with the Student Acceptable Use Agreement, which they will be expected to sign before being given access to IT systems;
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Will be expected to know and understand The BRIT School policies on the use of mobile devices;
- Must know and understand school policies on the taking / use of images and on cyber-bullying;
- Should 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/Carers

Parents and carers are responsible for:

- Endorsing the Student Acceptable Use Policy;
- Reading any and all policies relating to their child's use of IT.

Policy Statements

Education - Students

The education of students 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.

Online-Safety education is provided in the following ways:

- Key online-safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students are taught in lessons to be critically aware of the materials/content they access online, and are guided to validate the accuracy of information. Students are helped to understand the need to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- All students must agree to and sign the school's IT Acceptable Use Policy (see *Appendix. b*.). A copy of the Acceptable Use Policy is available on the School Website, in the Student Area.
- Staff should act as good role models in their use of IT, the internet and mobile devices.

Further information for teenagers can be obtained from the following external organisations:

- National Crime Agency/CEOP - https://www.thinkuknow.co.uk/14_plus/
- Childnet - http://www.childnet.com/young-people/secondary
- Childline - https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/

Education – Parents/Carers

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.

The BRIT School will therefore seek to provide information and awareness to parents and carers through:

Workshops, Letters, newsletters, website, Parents' forum.

Further information for parents can be obtained from the following external organisations:

- National Crime Agency/CEOP - https://www.thinkuknow.co.uk/parents/
- Childnet - http://www.childnet.com/parents-and-carers
- London Grid for Learning - https://www.lgfl.net/online-safety/resource-centre?s=16

Education and Training –Staff and Governors

It is essential that all staff receive online-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online-safety training will be made available to staff.
- An audit of the online-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online-safety as a training need within the approved process.
- This Online-Safety policy and its updates will be presented to and discussed by staff in team meetings.
- Governors should take part in online-safety training.

Further information for staff and governors can be obtained from the following external organisations:

- National Crime Agency/CEOP - https://www.thinkuknow.co.uk/teachers/
- Childnet - http://www.childnet.com/teachers-and-professionals
- London Grid for Learning - https://www.lgfl.net/online-safety/resource-centre?s=16

Handling Incidents

The BRIT School will take all reasonable precautions to ensure online safety.

- Staff and student are given information about infringements in use and possible sanctions.
- The pastoral team acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator 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).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" Publication is used as a framework for handling a sexting/nude selfie incident (*See Appendix. c. for further information*). This extract gives the initial actions that will be taken.

There will always be an initial review meeting, led by the Designated Safeguarding Lead (DSL). This will consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people;
  When assessing the risks the following will be considered:
  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Does the young person understand consent?
  - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care;
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed;
- What further information is required to decide on the best response;
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown;
- Whether immediate action should be taken to delete or remove images from devices or online services;
- Any relevant facts about the young people involved which would influence risk assessment;
- If there is a need to contact another school, college, setting or individual;
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved.

An immediate referral to police and/or children's social care will be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns become known).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Reviewing and Monitoring Online Safety

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, Behaviour Policy, Acceptable Use Policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

The IT Infrastructure

Password Security

Introduction

The BRIT School will be responsible for ensuring that the network is as safe and secure as is reasonably possible, and that:

- Users can only access data to which they have right of access;
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies);
- Access to personal data is securely controlled in line with the school's data protection policy (*see Appendix d.*) and the school's Privacy Statement (*see Appendix. e.*);
- Logs are maintained of access by users and of their actions while users of the system.

Responsibilities

The management of the password security policy will be the responsibility of the IT Support Team.

All users (staff and students):

- Will have responsibility for the security of their username and password;
- 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;
- Must immediately report any suspicion or evidence that there has been a breach of security.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- Through the school's online-safety policy and password security policy;
- Through the Acceptable Use Agreement.

Students will be made aware of the school's password policy:

- In tutorial / pastoral activities and/or e-safety assemblies;
- Through the Acceptable Use Agreement.

All users will have clearly defined access rights to The BRIT School's IT systems. Details of the access rights available to groups of users will be recorded by the IT Support Department and will be reviewed, at least annually, by the Online-Safety Working Group. 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).
- Authentication process should protect against brute force attacks.
- Passwords shall not be displayed on screen.
- Authentication shall be encrypted.
- Only IT support staff will have access to change staff passwords.
- All users will use unique accounts to support accountability.

Filtering

Introduction

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. However, the filtering system cannot provide a 100% guarantee that it will do so. Therefore, the school has a filtering policy to manage the associated risks and to provide preventative measures, which are relevant to the situation in this school.

The current system provides two tiers of defence. The major part of the web filtering is provided by our internet service appliance, which filters the whole network and is not dependant on any software installed on the workstation. This is 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 the classroom teacher to layer on additional white and black listings, and suspend internet access for individual students.

Responsibilities

The responsibility for the management of the filtering policy will be held by the online-safety coordinator. They will manage the school filtering, in line with this policy, and will ensure logs of changes and breaches of the filtering systems are kept by the IT Support Department.

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.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems, which are in place to prevent access to such materials.

A full list of what is filtered/blocked by the school and why can be found in the IT Network Filtering Policy (*see Appendix. f.)*.

Education / Training Awareness

Students will be made aware of the importance of filtering systems through the online-safety education programme (e.g. in Tutor groups and through assemblies). They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Policy (AUP)
- induction training
- Inset

Parents will be informed of the school's filtering policy through the Acceptable Use Guidance and through occasional online-safety awareness publications.

Changes to the Filtering System

Staff users may request changes to the filtering with an email request to the online-safety coordinator.

There should be strong educational reasons for changes and these changes may be for specific groups of users. The changes may be rejected for technical reasons due to the limitations of filtering systems as well as judgements about the appropriateness of materials.

All changes (and requests for change) must be logged by the IT support staff.

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 shared and FOLDR) 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 that will report and record any inappropriate use and keywords. Screen shots and screen recordings are taken of inappropriate usage.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The Principal
- SLT
- IT Strategy Group
- Governors on request

The filtering policy (see appendix. F) will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Infrastructure and Equipment for filtering and monitoring

The BRIT School's IT Support Department will be responsible for ensuring that the infrastructure and network is as safe and secure as is reasonably possible.

- There will be regular reviews and audits of the safety and security of The BRIT School IT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the IT Support and will be reviewed, at least annually, by the Online-Safety Team.
- All users will be provided with a username and password by the IT Support Team who will keep an up-to-date record of users and their usernames.
- Requests from staff for sites to be removed from the filtered list will be considered by the Online-Safety Coordinator.
- The IT Support staff regularly sample record the activity and documents of users on the school IT systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools will be used by staff to control workstations and view users' activity.
- A system will be developed for users to report any actual / potential online-safety incident to the IT Support Team, by using the 'Confide' System.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The downloading of executable files by users is not allowed.
- Staff are not permitted to install programmes on school workstations / portable devices.
- The infrastructure and individual workstations are protected by up-to-date antivirus software.

Email Systems & Provision

The BRIT School will:

- Use anonymous or group e-mail addresses, for example info@brit.croydon.sch.uk, and class email addresses;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;
- 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.

Staff

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.

Students

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

School Website

The Principal, supported by the Director of Communications and the Director of IT, takes overall responsibility to ensure that:

- The website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use students' names when saving images in the file names or in the tags when publishing to the school website.

Online Environments

Photographs and videos uploaded to the school's online environment (Planet eStream) will only be accessible by members of the school community;

In school, students are only able to upload and publish within school approved 'Online' systems, using school provided accounts.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At The BRIT School:

- The Head Teacher is the Senior Information Risk Officer (SIRO);
- We ensure staff know who to report any incidents where data protection may have been compromised;
- All staff are DBS checked and records are held in a single central record.

Technical Solutions

- Staff have secure area(s) on the network and online storage to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce 'log off' after an extended period.
- All servers are in locked and secure locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website - http://www.environment-agency.gov.uk/business.
- Where any protected or restricted data has been held we obtain a certificate of secure deletion for any server that may have contained personal data.
- We monitor and maintain logs of file deletion.

Equipment and Digital Content

Mobile Devices (Mobile phones, Tablets and other mobile devices)

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile devices.
- Mobile devices must not be used in certain areas within the school site, e.g. changing rooms and toilets.
- 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.
- All visitors are requested to switch off all mobile devices when in performances or presentations.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Principal. All mobile device use is to be open to monitoring scrutiny and the Principal is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.

Social Networking

Staff, Volunteers and Contractors

- Staff are instructed to keep professional and private communication separate.
- Teachers 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.

School staff will ensure that in private use:

- No reference should be made in social media to students, parents/carers or school staff;
- School staff should not be online friends with any current student. Any exceptions must be approved by the Principal. This does not apply to former students/alumni.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school, and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Students:

- Are taught about social networking, acceptable behaviours and how to report misuse intimidation or abuse, through our online safety tutorial work.
- Students are required to sign and follow our IT Acceptable Use Agreement.

Parents:

- Are reminded about social networking risks and protocols through communications materials when required;
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

The school maintains the right 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

In The BRIT School:

- We 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 (or annually);
- 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 about how images can be manipulated in their online safety education programme;
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;
- 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;
- Students are taught about what to do if they are subject to bullying or abuse.

Appendix.

a. Staff IT Acceptable Use Policy
b. Student IT Acceptable Use Policy
c. UKCCIS "Sexting in schools and colleges"
d. Data Protection Policy Statement
e. Privacy Statement