Created: March 2017
Last reviewed: Jan 2020

BST e-Safety Policy

The British School in Tokyo
School Policy Document

BST e-Safety Policy

Introduction

The development and expansion of the use of IT has transformed learning in schools in recent years. It is clear that young people will need to develop high levels of competency, to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that IT can bring to teaching and learning and schools around the world have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are certainly perceived to outweigh the risks. However, schools must, through their e-safety policy, ensure that they meet their obligations to ensure that children are safe and are protected from potential harm, both within and outside school. A recent Government initiative in March 2017 has been tasked with preventing children and young people from harm online and making the internet a safer place. The Green paper report is expected to be published this summer and will help inform any future planning.

The BST e-Safety Policy is intended to consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as our Safeguarding and Child Protection, Behaviour and Anti-Bullying policies.

UK national guidance suggests that it is essential for schools to take a leading role in e-safety. The British Educational Communications and Technology Agency (Becta), in its *Safeguarding Children in a Digital World*, recommends that:

> 'All schools have acceptable use policies, and ensure that parents are aware of the procedures for e- safety within the school. Recognising the growing trend for home-school links and extended school activities, furthermore schools should take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too.'

The Byron Review *Safer Children in a Digital World* stressed the central role of schools:

> 'One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area.'

Due to the ever changing nature of Information and Communication Technologies, it is best practice that the school reviews the e-Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

A useful source of updated information from the UK to guide review is the CEOP website:

http://www.thinkuknow.co.uk/Teachers/

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy is intended to help to ensure safe and appropriate use. The development and implementation of our strategy at BST involves all the stakeholders in a child's education from the Principal and Trustees to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- Phishing attacks
- The sharing/distribution of personal images without an individual's consent or knowledge (sexting, sextortion)
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Security vs convenience
- Access to unsuitable video/Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Impact of media on a person's perception about what people should look like
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other relevant school policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

All schools must demonstrate that they provide the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how BST aims to achieve this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational purposes.

Development / Monitoring / Review of this Policy

This e-Safety policy has been developed and will be monitored and reviewed by:

- The School e-Safety Officers (Secondary James Thomas; Primary Stephen Pritchard)
- Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- A designated Trustee
- Parents and Carers
- Independent Internet Safety Consultant

Consultation with the whole school community will take place regularly through:

- Staff meetings
- Student Council
- INSET and CPD
- Trustees' meetings
- Parents evenings and workshops
- BST website and newsletters

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Board of Trustees on:	March 2017
The implementation of this e-safety policy will be monitored by:	e-Safety Officers, Head Teachers and the designated Trustee.
Monitoring will take place at regular intervals:	At least once a year
The Educational Sub-Committee of the Board of Trustees will receive a report on the implementation of the e-Safety Policy:	At least once a year
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	January 2021

The school will monitor the impact of the policy using:

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

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 school ICT systems, both in and out of school.

The School has a responsibility, 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 e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

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 e-safety behaviour that take place out of school.

Roles and Responsibilities

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

Trustees
Trustees are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about e-safety incidents and monitoring reports. A member of the Board of Trustees, James Hollow, has taken on the role of *e-Safety* Trustee. The role of the e-Safety Trustee includes:

- *regular meetings with the e-Safety Officers*
- *regular monitoring of e-safety incident logs*
- *reporting to the Board of Trustees*

The Principal, Heads of School and Senior Leaders

- The Principal and Heads of School are responsible for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety will be delegated to the e-*Safety Officers*.
- The Heads of School are responsible for ensuring that the e-Safety Officers and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Heads of School will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the E-Safety Officer.

The Principal, Heads of School and all members of the Senior Management 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.

e-Safety Officers (Secondary James Thomas; Primary Stephen Pritchard)

- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff is aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the School's IT Manager and technical staff
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- meet regularly with e-Safety Trustee to discuss current issues and review incident logs
- attend relevant committee meeting of Trustees
- report regularly to the appropriate Senior Management Team

IT Manager / Technical staff:

The IT Manager is responsible for ensuring:

- that the School's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the School meets the e-safety technical requirements outlined in the latest UK e-Safety statutory guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- 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 he/she keeps up to date with e-safety technical information in order to effectively carry out the e-safety role and to inform and update others as relevant
- that the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-Safety Officer for investigation
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are all responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy Agreement (AUP)
- they report any suspected misuse or problem to the e-Safety Officer/Head of School for investigation/action/sanction
- digital communications with students should be on a sensible professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and copyright violations

- they monitor ICT activity in lessons, extracurricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- where Internet use is pre-planned students should be guided to sites suitable for their use; processes should be in place for dealing with any unsuitable material that is inadvertently found

The Child Protection Officers

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

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

E-Safety Committee

Members of the *e-safety committee* will assist the e-Safety Officer with:

- the production/review/monitoring of the school e-safety policy and related documents.

Students:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the School's e-Safety policy covers their actions out of school, if related to their membership of BST.

Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet, social media and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The School will therefore take every opportunity to help parents understand these issues through parents' evenings and workshops, newsletters, letters, website and social media.

Parents and carers will be responsible for:

- **endorsing (by signature) the Student Acceptable Use Policy**

Policy Statements

Education – staff and students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is, therefore, an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

e-Safety education will be provided in the following ways:

- An age-appropriate e-safety programme should be provided as part of ICT/Well-being/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/ pastoral activities
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Staff should always act as good role models in their use of ICT, the Internet and mobile devices

Education – parents / carers

Some parents and carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences. Parents sometimes either underestimate or do 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. 'There is a generational digital divide.' (Byron Report)

BST will, therefore, seek to provide information and awareness to parents and carers through:

- Letters, newsletters, BST website, BST social media accounts
- Parents evenings and workshops

Education & Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e- safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- The e-Safety Officers will receive regular updates through attendance at information/training sessions, participation in on-line training sessions and by reviewing guidance documents released by a broad range of providers, including COBIS.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings and on INSET days.
- The e-Safety Officer will provide advice/guidance/training to individuals as required.

Training – Trustees

Trustees should take part in e-safety training/awareness sessions, with particular importance for those who are members of the Education Subcommittee. This may be offered in a number of ways, including participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring

The School will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- BST ICT systems will be managed in ways that ensure that the school meets as closely as possible the e-safety technical requirements outlined in the latest UK guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located with restricted physical access
- **All users will have clearly defined access rights to school ICT systems.** Details of the access rights available to groups of users will be recorded by the IT Manager and will be reviewed, at least annually with the e-Safety Officers.
- **All users will be provided with a user name and password** by the IT team who will keep an up to date record of users and their user names. Users will be required to change their password regularly.
- The *master/administrator* passwords for the school ICT system, used by the IT Manager, must also be available to the Bursar or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their user name and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- BST has provided enhanced user-level filtering through the use of the Cisco ASA firewall, the Cyberoam UTM and the Bluecoat ProxySG web-based filtering software.
- In the event of the IT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal and Bursar.
- Any filtering issues should be reported immediately to the e-Safety Officers.
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager and the appropriate Head of School or Deputy. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the e-Safety Officer
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the IT Manager/ESO (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- An agreed policy is in place for the provision of temporary access of guests (eg visiting trainers, visitors) onto the school system.
- Agreed guidelines are in place regarding the extent of personal use that users (staff and students) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed procedure is in place that allows staff to have programmes installed on school workstations/portable devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

e-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where Internet use is pre-planned, it is best practice that students should be 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.
- Where students are allowed to freely search the Internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the IT Manager (in consultation with the relevant Head/Deputy) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the Internet.

Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or long term. There are many reported incidents of employers/universities carrying out Internet searches for information about potential and existing employees.

The Safer Internet Day organization carried out a survey in 2017 specifically looking into the digital lives of young people aged 8-17 and the role that images play in it. At the time the survey took place 1 in 6 children had shared a photo online in the last hour and 1 in 8 children had shared a selfie in the last day. Even more alarmingly nearly half of the children surveyed were worried about how attractive they look when they share a photo online, pointing to a culture obsessed with body image.

The school will inform and educate users about the risks of sharing images online and the influence that media has on people's perception of body image and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet, eg on social networking sites.

- Members of staff are permitted to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should usually be captured and stored on school equipment; staff should avoid using personal equipment for such purposes where possible.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- **Students' full names should not be used anywhere on a website or blog, particularly in association with photographs.**

Data Protection

Personal data will be recorded, processed, transferred and made available according to the UK Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password-protected computers and other devices, ensuring that they are properly logged-off at the end of any session in which they are using personal data.
- Transfer sensitive personal data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (note that many memory sticks/cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

Communication Technologies

When using communication technologies the school considers the following as good practice:

- The official BST email service may be regarded as safe and secure and is monitored
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy – the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- **Any digital communication between staff and students or parents/carers must be professional in tone and content.** These communications should only take place on official (monitored) school systems. Personal email addresses or social media accounts must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses of members of staff should be published.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other ICT systems. Other activities eg cyber-bullying are banned and could lead to criminal prosecution. There are however a range of activities that may generally be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Please refer to the BST Acceptable Use Guidelines for further information.

Paul Tough
Principal