



7f Acceptable use (IT) Policy

1. Statutory Policies	2. Notice Policies
Author Led	Headmaster
Date of Review	July 2025
Next Review	June 2026
Comment	Annual Review
Website	Yes

BISC Mission Statement

To build on the proven quality of the British curriculum whilst fostering an international perspective towards education.

To deliver academic excellence and create an inspiring place for children and young people to act and achieve the best version of themselves.

'Aspire, Act, Achieve'

Purpose and Scope of Policy

Although our host country is not bound by UK statutory law, as an International British School, this policy has been written taking into account UK statutory guidance 'Keeping Children Safe in Education' 2024 and 'Working Together to Safeguard Children' 2024

The purpose of this policy is to:

- Safeguard and protect all members of the BISC community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practices when using technology.
- Identify clear procedures to use when responding to online safety concerns.

The policy is written to assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practices. It aims to set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.

BISC identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content** - being exposed to illegal, inappropriate or harmful material.
- **Contact** - being subjected to harmful online interaction with other users.
- **Conduct** - personal online behaviour that increases the likelihood of or causes harm.

At BISC we believe that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life and believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including The Board, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services to the school (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

Online safety is essentially about creating a safe environment when using IT. This includes the use of the internet and social networking sites. This document is intended to outline the school's approach to preventing safeguarding issues, including cyber-bullying, as well as detailing how we respond to e-safety issues when they emerge.

Roles and responsibilities

The Board

The Board has overall responsibility for monitoring this policy and holding the principal to account for its implementation. The Board delegates responsibility to The Headmaster / DSL to organise meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All board members will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms of acceptable use of the school's ICT systems and the internet.
- Approve the Online Safety Policy and review the effectiveness of the policy.

The Headmaster

The Headmaster is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The Headmaster:

- Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance.
- Take overall responsibility for online safety provision.

- Ensure suitable 'risk assessments' undertaken so the curriculum meets the needs of students, including risk of children being radicalised.
- To ensure Board Members are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.

The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) roles and responsibilities are set out in our Child Protection and Safeguarding Policy. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headmaster in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headmaster, IT Director and other staff, as necessary, to address any online safety issues or incidents.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- To ensure that online safety incidents are logged as a safeguarding incident.
- Oversee any student surveys / student feedback on online safety issues.
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school Safeguarding and Child Protection Policy.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headmaster and/or The Board.

The IT Director

The IT Directors is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).
- To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To model safe, responsible and professional behaviours in their own use of technology.
- Agreeing and adhering to the terms of the policy for Acceptable Use of ICT systems and the internet and ensuring that students follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's Behaviour and Safeguarding and Child Protection Policies.
- At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to login and allow a factory reset.

Parents

Parents are expected to:

- Notify a member of staff or the Headmaster of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms on Acceptable Use of the school's ICT systems and the internet and the BYOD policy.
- To support the school in promoting online safety and acknowledge the supporting policies designed to promote this.

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms of Acceptable Use.

Educating students about online safety

Students will be taught about online safety as part of the curriculum. The text below is taken from the National Curriculum computing programmes of study:

Key Stage 1 students will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

Key Stage 3 students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Key Stage 4 & 5 will be taught to:

- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- Understand the implications of their digital identity moving forward into higher education and careers.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. Online safety will also be covered during parents' meetings. If parents have any queries or concerns in relation to online safety incidences, these should be raised in the first instance with the Headmaster and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Headmaster.

Cyberbullying

Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour and Safeguarding and Child Protection policies.)

Preventing and addressing cyberbullying

To help prevent cyberbullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal, Social, Health, Citizenship and Economic (PSHCE) education, and other subjects where appropriate. All staff, Board members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

In relation to a specific incident of cyberbullying, the school will follow the processes set out in the Acceptable Use Policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power as outlined under the UK Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. Although we are not in the UK, BISC prides itself on adhering to UK standards for education and pastoral care.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules.

If inappropriate material is found on the device, it is up to the DSL, in conjunction with the Headmaster, to decide whether they should:

- Delete that material.
- Retain it as evidence (of a criminal offence or a breach of school discipline).
- Report it to the police.
- Any searching of students will be carried out in line with the latest guidance on screening, searching and confiscation.
- Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school Complaints Procedure which is available on the school website.

Acceptable use of the internet in school

All students, parents, staff, volunteers and Board members are expected to sign an agreement regarding the Acceptable Use of the school's IT systems and the internet. These can be found in the IT and Acceptable Use Policy. Visitors will be expected to read and agree to the school's terms on Acceptable Use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, Board members and visitors (where relevant) to ensure they comply with the above. More information is set out in the Acceptable Use Policy.

Students and Staff using mobile devices in school

Any use of mobile devices in school by students or staff must be in line with the Acceptable Use Policy and Agreements. Any breach of the Acceptable Use Agreement by a student may trigger disciplinary action in line with the school's Behaviour Policy, which may result in the confiscation of their device.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in the IT and Acceptable Use Policy. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the IT director.

How the school will respond to issues of misuse

Where a student misuses the school's IT systems or internet, we will follow the procedures set out in the Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff Disciplinary Procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents should be reported to the police.

Training

All staff members will receive training on safe internet use and online safeguarding issues including cyberbullying and the risks of online radicalisation. All staff members will receive additional training as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Board members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the Headmaster.

Links to other relevant school policies

- 1- Anti Bullying
- 2- Safeguarding and Child Protection
- 3- Staff Code of Conduct
- 4- Behaviour and Discipline
- 5- Acceptable Use
- 6- Complaints procedure
- 7- BYOD