E-Safety Policy

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at International British School of Bucharest with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of International British School of Bucharest.
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope

This policy applies to all members of International British School of Bucharest community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of International British School of Bucharest.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school / academy* 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 outside of the school / academy, but is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

This online safety policy has been written by the school with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', 'Working Together to Safeguard Children' 2018.

When the International British School of Bucharest is operating in response to coronavirus (Covid-19); our safeguarding principles in accordance with 'Keeping Children Safe in Education' (KCSIE) and related guidance, remain the same. Where children are asked to learn online at home in response to a full or partial closure, will follow expectations as set out within the Child Protection Policy and in line with DfE Guidance, 'Safeguarding and remote education during coronavirus (COVID-19)' 2020.

The International British School of Bucharest 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.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-Safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)

e-Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• promotes an awareness and commitment to e-safeguarding throughout the school community
	• ensures that e-safety education is embedded across the curriculum
	• liaises with school ICT technical staff
	• To communicate regularly with SLT to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
	• To ensure that an e-Safety incident log is kept up to date
	• facilitates training and advice for all staff
	• liaises with relevant agencies
	• Is regularly updated in e-safety issues and legislation, 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 adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly

Role	Key Responsibilities
Network Manager/technician	• To report any e-Safety related issues that arises, to the e-Safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • that the use of the *network / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be 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 • To report any suspected misuse or problem to the e-Safety coordinator • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Role	Key Responsibilities
Pupils	• to know and understand school policy on the use of Bring Your Own Device • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To 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 the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies
Parent Liasion Officer	• Educating Parents and raising awareness as instructed by Head.
Parents/carers	• to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images • to read, understand and promote the school Whole School Use of Digital Devices Policy and Whole School Bring Your Own Device Policy with their children • to access the school website / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Communication

How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/staffroom/ classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints

- The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by tutor / Head of Year / e-Safety Coordinator / Headteacher;

  - informing parents or carers;
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - referral to Police/Relevant Authority.
- Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

Review and Monitoring

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and other stakeholders. All amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-Safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
  - to STOP and THINK before they CLICK
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know how to narrow down or refine a search;
  - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - to understand why they must not post pictures or videos of others without their permission;
  - to know not to download any files – such as music files - without permission;
  - to have strategies for dealing with receipt of inappropriate materials;

  - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
  - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
  - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher, or trusted staff member, the local police or an international organisation such as www.childnet.com

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program through annual updates/ termly staff meetings etc.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets; in school newsletters; on the school web site;
  - demonstrations, practical sessions held at school when appropriate;
  - suggestions for safe Internet use at home;
  - Provision of information about national support sites for parents.

Management of Learning Platforms and Systems

- The Senior Leadership Team and staff will regularly monitor the usage of the International British School of Bucharest learning platforms and systems by students and staff in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised about acceptable conduct and use when using the International British School of Bucharest learning platforms and systems.

- Only members of the current student, parent/carers and staff community will have access to the International British School of Bucharest platforms and systems.
- All users will be mindful of copyright issues and will only upload appropriate content onto the portal.
- When staff and students leave the International British School of Bucharest their account or rights to specific International British School of Bucharest areas will be disabled.
- Any concerns about content on the International British School of Bucharest platforms and systems may be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - The material will be removed by the site administrator if the user does not comply.
    - Access to the platforms/systems for the user may be suspended.
    - The user will need to discuss the issues with a member of Senior Leadership Team before reinstatement. A student's parent/carer may be informed.
    - A visitor may be invited onto the portal by a member of the Senior Leadership Team. In this instance there may be an agreed focus or a limited time slot.
    - Students may require editorial approval from staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

Official use of social media

- Official use of social media sites by International British School of Bucharest will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the head teacher.
- Official International British School of Bucharest social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use International British School of Bucharest provided email addresses to register for and manage official International British School of Bucharest approved social media channels.
- Staff running official International British School of Bucharest social media channels will ensure that they are aware of the required behaviours and expectations of use. They will ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official International British School of Bucharest social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official International British School of Bucharest social media sites will comply with legal requirements will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by International British School of Bucharest will be in line with existing policies, including: anti-bullying and child protection.
- Images or videos of students will only be shared on official International British School of Bucharest social media sites/channels in accordance with International British School of Bucharest's Photographic Image Use policy.
- Information about safe and responsible use of International British School of Bucharest social media channels will be communicated clearly and regularly to all members of the International British School of Bucharest community.
- Official social media sites, blogs, or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the International British School of Bucharest website and take place with written approval from Senior Leadership Team.
- Senior Leadership Team staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.

- Parents/carers and students will be informed of any official International British School of Bucharest social media use, along with expectations for safe use and International British School of Bucharest action taken to safeguard the community.
- The International British School of Bucharest official social media channels are:
    - The school website
    - IBSB Facebook page
    - IBSB Instagram account
    - IBSB Twitter account
- Public communications on behalf of International British School of Bucharest will, where possible, be read and agreed by at least one other colleague.
- An account will link back to International British School of Bucharest's website and/or Acceptable Use Policy to demonstrate that the account is official.
- The International British School of Bucharest will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Student's use of social media

- Safe and responsible use of social media sites will be outlined for students and their parents as part of International British School of Bucharest's Acceptable Use Policy.
- Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites, which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, International British School of Bucharest attended, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs, etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with students and written parental consent will be obtained, as required.
- Any official social media activity involving students will be moderated by International British School of Bucharest where possible.
- International British School of Bucharest is aware that many popular social media sites state that they are not for children under the age of 13, therefore, International British School of Bucharest will not create accounts within the school specifically for students under this age.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at International British School of Bucharest, will be dealt with in accordance with existing International British School of Bucharest policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

Expectations for safe use of personal devices

Electronic devices of all kinds that are brought into International British School of Bucharest are the responsibility of the user at all times. The International British School of Bucharest accepts no responsibility for the loss, theft or damage of such items. Nor will International British School of Bucharest accept responsibility for any adverse health effects caused by any such devices either potential or actual.

The sending of abusive or inappropriate messages or content via digital devices is forbidden by any member of the International British School of Bucharest community. Any breaches will be dealt with as part of the International British School of Bucharest Staff Code of Conduct and student Behaviour for Learning Policies.
All members of the International British School of Bucharest community will be advised to take steps to protect their digital devices from loss, theft, or damage.
All members of the International British School of Bucharest community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
All members of the International British School of Bucharest community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the International British School of Bucharest policies.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse, or access to inappropriate materials and know how to do so
- 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 the school
- 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

Staff:

- are responsible for reading the school's E-safety Policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.
- are responsible for checking and approving YouTube videos prior to sharing them with students

Students/Pupils:

- are responsible for using the school wifi, school digital devices, and byod digital devices in accordance with school policy
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers:

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- if incidents occur, they are recorded on the school's CPOMS system
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues ANY ROMANIAN EQUIVALENT?
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders.
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school:

- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of anti-virus software and network set-up so staff and pupils cannot download executable files;
- Uses approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or Google Classroom
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;

- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment or approved blogging sites
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of Google Classroom as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search , …..
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the system administrator. Our system administrator(s) logs or escalates as appropriate to the Technical service provider as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying, etc., available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- *Has additional local network auditing software installed;*
- Storage of all data within the school will conform to data protection requirements
  - Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. From Year 6 they are also expected to use a personal password;
- All pupils have their own unique username and password which gives them access to the Internet and Google Classroom
- Pupils will be provided with their own school approved email account;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;

- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 5 mins and have to re-enter their username and password to re-enter the network.];
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 6 o'clock to save energy;
- Has set-up the network so that users cannot install executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / approved systems:
  e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides pupils and staff with access to content and resources through Google Classroom
- which staff and pupils access using their username and password
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;

- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, every 90 days / twice a year

E-mail

This school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Provides *highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils*; uses Google accounts with students as this has email content control
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- We use anonymous or group e-mail addresses, for example info@ibsb.ro or admissions@ibsb.ro, for communication with the wider public.
- Share staff email addresses with parents at the start of each year and in the New Parent Handbook
- 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.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Year R/1 pupils are introduced to principles of e-mail through Google Classroom or closed 'simulation' software.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;

- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments;
- embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

Staff:

- Staff should only use the e-mail system provided by the school for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: FLORIN GHITA
- The school web site complies with the UK statutory DfE guidelines for publications;
- 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;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admissions@schooladdress. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Social networking

- 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.
- The school's preferred system for social networking will be maintained in adherence with the communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- 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 *International British School of Bucharest* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners In the E-safety Folder on the School Server
- 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 one central record

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  - staff
  - governors
  - pupils
  - parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.

- School staff with access to setting-up usernames and passwords for email, network access and Google Classroom access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after <5 mins idle time>.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use named alternative solution for disaster recovery on our network / admin, curriculum server(s).
- We comply with the WEEE directive on equipment disposal> by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and <get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.
- We are using secure file deletion software.

6. Equipment and Digital Content

- School provides Android Tablets and laptops to a number of teaching staff for administrative purposes and to help with the planning of Tablet based lessons.
- Staff sign an agreement on receipt of a device which can be found as an appendix to this document.

Personal mobile phones and mobile devices use by staff and visitors

- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff should be aware that the school Wifi is intended for school use and should now be used for personal purposes
- Staff mobile phones which are brought into school must be stored out of sight on arrival at school. They must remain in silent mode until the end of the school day. Staff members may only use their phones for personal purposes during school break times.

- Mobile phones and personally owned devices should not be used for personal use during lessons. They should be switched off or turned onto silent.
- All visitors are requested to keep their phones on silent.
- The recording, taking, and sharing of images, video, and audio on any mobile phone is to be avoided by staff and visitors; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored. All mobile phone use is to be open to scrutiny and the head teacher may withdraw or restrict authorisation for use at any time if deemed necessary.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, or carers, then a school mobile phone will be provided and should be used.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- In an emergency where a staff member doesn't have access to a school-owned device, they may use their own device and where possible hide their own mobile number for confidentiality purposes.
- Mobile phones and personally-owned digital 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 phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- The Bluetooth or similar function of a mobile phone should be switched off at all times during school hours.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If they are brought into school, they will be handed in during the morning registration period. They will be then stored securely before being returned at the end of the day.
- The School is not responsible for any damage incurred whilst on the School premises.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy at the end of the school day.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone 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.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone for students enrolled up to Y11. Y12 & 13 students may, however, go to the Sixth Form College office to use their phone under the supervision of a member of staff.
- 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.
- Students will be provided with school digital devices to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence, or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.

Digital images and video in 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;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- The school's Whole School Use of Digital Devices Policy includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their eSafety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils 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.
- Pupils 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 identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

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.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

Related Polices

PS/SS Behaviour for Learning Policy
PS Computing Policy
PS/SS Curriculum Policy
PS/SS PSHE Policy
Secondary School ICT Room Use Policy
Staff Recruitment and Contract Renewal Policy
Whole School Anti-bullying Policy
Whole School Bring Your Own Device Policy
Whole School Child Protection and Safeguarding Policy
Whole School Use of Digital Devices Policy

Document Control		
Draft Issued	August 2022	
Author/Editor	Marius Bogdan	
Draft Approval	Kendall Peet	Head Teacher
Signed off by	SLT	
Review Date	August 2024	
Review cycle	2 years	