British International School of Timisoara

We Provide the Foundation on Which Our Children Can Flourish

School Policies

E-safety policy

Approved by:	Head of School	Date: May 2019
Last reviewed by:	School Leadership Team	Date: June 2024
Next reviewed by:	School Leadership Team	Date: June 2025

E-safety policy

General

British International School of Timisoara is a coeducational private international school offering a British-style education and accepting children aged between 4 and 18.

British International School of Timisoara offers its students a truly international experience through a British-style curricula and adheres to the guidelines of the Council of British International Schools, Cambridge Assessment International Education and the International Baccalaureate Organisation. Our qualified, internationally experienced and dynamic educators teach all subjects in English, with the exception of the lessons of Romanian, which are being taught by qualified and engaging local teachers.

Our Vision

We provide the Foundation on which our Children can Flourish
Inspiring our students to Learn and Live with Purpose

Our Mission

Building a community of learners where students are given meaningful opportunities to learn, experience, grow, succeed and excel in all areas of their academic and personal development

Our Core Values

We Think, We Explore and We Learn
We Listen, We Respect and We Care
We Speak Up, We Participate and We Strive

At BIST we want to ensure that all members of our community understand and adhere to our school ethos and values. Rules and regulations will be in place to protect all members of the community and to give everyone equal opportunities for development and progress.

Introduction

Children of our generation develop skills in technology better than many adults. The IT world in its many forms has become an integral part of our day-to-day life and has brought a lot of benefits and challenges in our world and more specifically in education. Having access to technology in the classroom gives students different ways to learn and helps them develop various skills. Teachers use technology to come up with creative ways to keep children engaged and support the learning process. Used appropriately with teacher's guidance as a mean to support progress and understanding, technology in the classroom can make the teaching and learning experience more meaningful and fun.

At BIST technology will be part of the curriculum and will be used to support the learning process. We will ensure to provide top quality IT resources (laptops, tablets, interactive whiteboards, etc…) in order to give our students, the best possible opportunities to learn and develop skills, but also to support those who wish to study Computer Science at advanced level and possibly build a career in the IT world.

As technology will be integral part of our life in BIST, E-safety will represent one of our main priorities.

This policy applies to all members of British International School of Timisoara 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 British International School of Timisoara.

Purpose

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at British International School of Timisoara with respect to the use of ICT-based technologies;
- safeguard and protect the children and staff of British International School of Timisoara;
- 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

The Education and Inspections Act 2006 empowers Heads of Schools 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The British International School of Timisoara 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.

BIST policy on approved IT devices in school

BIST will provide all the teachers and a number of non-teaching staff (school nurse, educational psychologist, admin staff working in the office, IT technician) with a MacBook. All teaching staff will also be provided with an iPad/MacBook. Members of staff sign an agreement on receipt of a device which can be found as an appendix to this document.

BIST will provide access to iPad/MacBook's during school time to all students in the Primary School. ICT/Computing lessons will take place in the ICT room equipped with desktops.

A Bring Your Own Device Policy (BYOD) will be implemented at the Secondary School stage. All students in years 7 to 13 will be allowed to bring their personal laptop to school, which will be used in school for educational purpose only and in line with the school polices and regulations. See BYOD policy for details on this aspect.

Most classrooms will be equipped with interactive panels and multipurpose smaller classrooms will be equipped with TV displays to be used with the MacBook's.

It is school policy to not allow students to bring to school smart phones and any other devices (tablets or other devices with internet connection or camera). If students chose to bring these devices to school, they will have to give them for safe keeping to the school office and collect them at the end of the school day. Consequently, there should be no opportunity for any student to use IT devices to take pictures or record anything in the school, except for those situations when there is a teacher guided activity and there are clear guidelines and supervision in place for the activity. Even in these circumstances, students may only use the school devices (iPad/MacBook's)

Staff use of personal devices

Members of staff will use their mobile phones (smart phones) with care and consideration during school time (not in lessons and not during break times) only for matter that can't be dealt with out of school time and ideally not in the presence of children. The Wi-Fi internet on the smart phones will be used taking into account all Safeguarding aspects and guidance in this policy.

- 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;
- staff will be issued with a school phone where contact with students, parents or carers is required;
- mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode; Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances;
- 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;
- if a member of staff breaches the school policy then disciplinary action may be taken;
- 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, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Communication

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

- Policy to be posted on the school website;
- 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;

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

Roles and responsibilities

School Management Team

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

E-Safety coordinator (Safeguarding)

- 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;
- will communicate regularly with SLT to discuss current issues, review incident logs and filtering / change control logs;

- will ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident;
- will 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

- will oversee the delivery of the e-safety element of the Computing curriculum
- will liaise with the e-safety coordinator regularly

IT technician

- will report any e-Safety related issues that arises, to the e-Safety coordinator;
- will 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;
- will ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date);
- will ensure the security of the school ICT system;
- will ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices;
- will ensure that the school's policy on web filtering is applied and updated on a regular basis;
- will keep up to date with the school's e-safety policy and technical information in order to effectively carry out his e-safety role and to inform and update others as relevant;
- will ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster;
- will keep up-to-date documentation of the school's e-security and technical procedures.

Data manager

- will ensure that all data held on pupils on the school office machines have appropriate access controls in place.

Teachers

- will embed e-safety issues in all aspects of the curriculum and other school activities;
- supervise and guide pupils carefully when engaged in learning activities involving online technology;
- will 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

- will read, understand and help promote the school's e-Safety policies and guidance;
- will read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy;
- will be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies regarding these devices;
- will report any suspected misuse or problem to the e-Safety coordinator;
- will maintain an awareness of current e-Safety issues and guidance e.g through CPD;
- will model safe, responsible and professional behaviours in their own use of technology;

- will 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.

Students

- will read, understand, sign and adhere to the Student Acceptable Use Policy (at KS1 it would be expected that parents / carers would sign on behalf of the pupils);
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials;
- will know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- will know and understand school policy on the use of mobile phones, digital cameras and handheld devices;
- will know and understand school policy on the taking / use of images and on cyber-bullying;
- will 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;
- must take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home;

Parents / carers

- will 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;
- will read, understand and promote the school Pupil Acceptable Use Agreement with their children;
- will access the school website / on-line student records in accordance with the relevant school Acceptable Use Agreement;
- will consult with the school if they have any concerns about their children 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.

Pupil e-Safety curriculum

BIST has a clear, progressive e-safety education programme as part of the Computing curriculum and PSHEE 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 to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

In addition, BIST will:

- plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network;
- will ensure staff will model safe and responsible behaviour in their own use of technology during lessons;
- will ensure 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;
- will ensure 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.
- will ensure 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 with information and guidance on the E-Safeguarding policy and the school's Acceptable Use Policies.

Parent awareness

BIST 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;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

Expected conduct

In BIST we expect **all users** to:

- be 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.);
- understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- 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;

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;
- know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Students:

- 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

At BIST:

- 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;
- 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;
- 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.

Managing the ICT infrastructure / Internet access, security (virus protection) and filtering

At BIST:

- we use 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;
- we use user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- we ensure network healthy through use of anti-virus software and network set-up so staff and pupils cannot download executable files;
- we use approved systems and secured email to send personal data over the Internet and we use encrypted devices or secure remote access where staff need to access personal level data off-site;
- we block all Chat rooms and social networking sites except those that are part of an educational network;
- we only unblock other external social networking sites for specific purposes / Internet Literacy lessons;
- we block pupil access to music download or shopping sites, except those approved for educational purposes at a regional or national level;
- we use security time-outs on Internet access where useful;
- we are vigilant in the supervision of pupils' use, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- we ensure all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- we ensure pupils only publish within an appropriately secure environment or approved blogging sites;
- we require staff to preview websites before use;
- we plan the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- we are vigilant when conducting 'raw' image search with pupils;
- we inform all users that Internet use is monitored;
- we inform staff and students that that they must report any failure of the filtering systems directly to the system administrator. Our system administrator logs or escalates as appropriate to the Technical service provider as necessary;
- we make clear that all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse, through staff meetings and teaching programme;
- we provide advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents;
- we immediately refer any material we suspect is illegal to the appropriate authorities.

Network management (user access, backup)

At BIST:

- we use individual, audited log-ins for all users;
- we use guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- we use teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- we have additional local network auditing software installed;

- storage of all data within the school will conform to data protection requirements;

To ensure the network is used safely, BIST:

- 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;
- ensures that staff access to the schools' management information system is controlled through a separate password for data security purposes;
- will provide pupils with an individual network log-in username. From Year 7 they are also expected to use a personal password;
- will ensure all pupils have their own unique username and password which gives them access to the Internet;
- will ensure all secondary school pupils will be provided with their own school approved email account;
- will make it clear that no one should log on as another user and will make it 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;
- will set-up the network with a shared work area for pupils and one for staff. Staff and pupils will be shown how to save work and access work from these areas;
- will require 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;
- 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;
- will set-up the network so that users cannot download executable files / programmes;
- will block access to music/media download or shopping sites, except those approved for educational purposes;
- will scan all mobile equipment with anti-virus / spyware before it is connected to the network;
- 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";
- maintains equipment to ensure Health and Safety is followed;
- 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;
- ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / approved systems:
- 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;
- 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;
- reviews the school ICT systems regularly regarding health and safety and security.

Passwords policy

At BIST we will make 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 and:

- 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

At BIST we will provide staff with an email account for their professional use and we want to make it clear that personal email should be through a separate account. At BIST:

- we do 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@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public;
- we 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;
- we will ensure that email accounts are maintained and up to date;
- we will report messages relating to or in support of illegal activities to the relevant Authority and if necessary, to the Police;
- we know 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.

Students

At BIST students are introduced to, and use e-mail as part of the ICT/Computing scheme of work:

- Year 1 pupils are introduced to principles of e-mail through 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.
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

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;
- All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- the School Management team 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;
- 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 admin@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 school 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.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- the Head of School is the Senior Information Risk Officer (SIRO);
- staff are clear who are the key contact(s) for key school information are;
- 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
    - 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 or network access are working within the approved system and follow the security processes required by those systems;
- we ask staff to undertake at least annual housekeeping 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 crosscut shredder / collected by secure data disposal service.

Digital images and video
In this 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;
- staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of 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.

Appendix 1

EMPLOYEE IT DEVICE ASSIGNMENT FORM

By completing and signing this form, I accept full responsibility for the device identified below. I have read, understood and agree to the school's E-Safety policy and the procedures listed in this document:

1. The device remains the property of the school.
2. The device may be used by the named employee, both on and away from school premises, within the bounds of the school's Acceptable Use of Technology Policy.
3. Personal use of the device is permitted outside of teaching hours within the bounds of the school's Acceptable Use of Technology Policy.
4. To protect the privacy of staff, students and visitors, employees are prohibited from using their device as a means to photograph and/or record an individual in any form without that individual's knowledge and consent.
5. Students will not be allowed unsupervised access to employee devices.
6. The device may be recalled at any time for maintenance and servicing.
7. Loss, damage or technical issues will be immediately reported to the ICT coordinator.
8. The device will not be left unattended and will be kept away from food and liquids. If left at school overnight it will be locked up in an appropriate place.
9. While an employee is not financially liable for a device, he/she agrees to take every necessary precaution to avoid loss or damage.
10. Employees using devices for network access will, without exception, use secure data management procedures. All devices will be protected by a strong password.
11. The school accepts no responsibility for the loss of personal data stored on a device.
12. Apps will not be installed or deleted without permission from the ICT coordinator. Any purchases made on or for the device must be approved by SLT.
13. The School is under no legal, financial or other obligation to provide a replacement device to any employee whose device is lost, stolen or damaged.
14. The School may add security and other tracking technology to any and all devices issued by it and any and all usage will be subject to management review, monitoring and auditing.
15. Non-compliance with any policies or procedures listed here may result in the withdrawal of technology privileges and/or other appropriate disciplinary action.

Device:

Employee Signature:

Date:

Authorised by:

Date:

Appendix 2

ACCEPTABLE USE POLICY (AUP) STAFF AGRREMENT FORM

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the SLT.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use".
- I will access school resources remotely (such as from home) only through school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will alert the school's named DSL or relevant senior member of staff if I feel the behaviour, in relation to their use of IT, of any child may be a cause for concern.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature (tick to confirm)

- I agree to abide by all the points above ☐
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies ☐
- I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems ☐

Signature ..... Date ……..

Full Name …… (printed)

Job title .....

School .....

Authorised Signature (Head of Primary School / Head of Secondary School)

I approve this user to be set-up.

Signature ..... Date……..

Full Name …….. (printed)

Appendix 3

KEY STAGE 1 AGRREMENT – for students

Think before you click	
S 	I will only use the Internet and email with an adult's permission
A 	I will only click on icons and links when I know they are safe
F 	I will only send friendly and polite messages
E 	If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

Appendix 4

KEY STAGE 2 AGRREMENT – for students

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything, I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

Appendix 5

SECONDARY SCHOOL AGRREMENT – for students

Secondary Pupil Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace. I will only edit or delete my own files and not view, or change, other people's files without their permission.
3. I will keep my logins, IDs and passwords secret.
4. I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies.
5. I will only e-mail people I know, or those approved by my teachers.
6. The messages I send, or information I upload, will always be polite and sensible.
7. I will not open attachments, or download a file, unless I have permission, or I know and trust the person that has sent them.
8. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
9. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
10. If I see anything, I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher / trusted adult.
11. I am aware that some websites and social networks have age restrictions and I should respect this.
12. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

I have read and understand these rules and agree to them.

Signed: *Date:*

Appendix 6

THE USE OF DIGITAL IMAGES AND VIDEO

Following the UK Data Protection Act 1998, we ask permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupil's work, we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity; e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.
- Your child's image being used for presentation purposes around the school; e.g. in class or wider school wall displays or PowerPoint© presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Appendix 8

THE USE OF SOCIAL NETWORKING AND ON-LINE MEDIA

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.