CITY OF BIRMINGHAM EDUCATION DEPARTMENT

BASKERVILLE SCHOOL

E-Safety Policy

Date reviewed: May 2016
Next review: May 2017

BASKERVILLE SCHOOL, FELLOWS LANE, HARBORNE, BIRMINGHAM, B17 9TS

TELEPHONE : 0121 427 3191
FAX : 0121 428 2204

VISION STATEMENT

We will ensure the entitlement of each student to access a variety of opportunities to promote academic, social, emotional and physical development.

We will use autistic specific, empathetic approaches and an autistic sympathetic learning environment to promote student learning and personal development.

We will provide choices and challenges in order to maximise potential and build upon strengths and interests.

All the members of the school community are valued equally and work in partnership with parents, carers and the wider community.

We will work within a supportive school framework to promote and celebrate individual success, integration into the wider community and prepare students for life after school.

All of the students at Baskerville School have autistic spectrum disorders; they have greater difficulty than other students with social understanding and communication. Therefore, it is essential that this policy be implemented consistently to support all students**.**

Young people with autism and other communication disorders often find internet communication easier than face to face communication.
On the internet people's use of consistent and easily recognisable emoticons replaces the need to decode people's body language, facial expressions and vocal tone that can be problematic in personal communications.

Internet-learning provides opportunities for learning through repetition that supports students who take longer to learn new things and embeds the learning they do in the classroom by undertaking activities as many times as they need to in order to consolidate their learning.

Alongside the many benefits to young people there are also a number of risks. With access to technology comes the potential for cyberbullying, online grooming and risk of exposure to inappropriate content. This is a risk for all young people using the internet but the risk can be more profound for young people with ASD as a result of increased vulnerability, tendencies towards obsessive compulsive behaviour and social naivety.

For this reason the requirement to ensure that students and young people are able to use the internet and related communications technologies appropriately and safely needs to be addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy has been developed to help ensure safe and appropriate use of ICT. The development and implementation of this strategy should involve all the stakeholders in a young person's education from the Head Teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

This policy has been written in conjunction with the following:

1. **Safeguarding policy**
2. Acceptable Use Agreement (Staff)
3. Acceptable Use Agreement (Students)
4. Behaviour Policy
5. Whistle blowing policy
6. Search and Confiscation guidance from DfE https://www.gov.uk/government/publications/searching-screening-and-confiscation
7. Mobile Phone policy

Baskerville 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 Baskerville School with respect to the use of ICT-based technologies;
- safeguard and protect the students and staff of Baskerville School;
- assist school staff working with students 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, violence and associated offensive language through ignoring age ratings in games, images of 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);
- (Ref Ofsted 2013).

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

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the Baskerville 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 Baskerville School, but is linked to membership of Baskerville 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.

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

Role	Key Responsibilities
Head Teacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • 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 ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To receive regular monitoring reports from the E-Safety Co-ordinator (Faculty Leader) • 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) • To ensure that all data held on students on the school's learning platform is adequately protected
E-Safety Co-ordinator (Faculty Leader) /Assistant Head Pastoral	• To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • To promote an awareness and commitment to e-safeguarding throughout the school community • To ensure that e-safety education is embedded across the curriculum • To liaise with school ICT technical staff • To communicate regularly with SLT and the designated e-safety Governor and committee to discuss current issues, review incident logs and filtering / change control logs • To ensure that an e-safety incident log is kept up to date • To facilitate training and advice for all staff • To liaise with the Local Authority and relevant agencies • To be regularly updated in e-safety issues and legislation and be aware of the potential for serious child protection issues to arise from: o sharing of personal data

Role	Key Responsibilities
	o access to illegal / inappropriate materials o inappropriate on-line contact with adults / strangers o potential or actual incidents of grooming o cyber-bullying and use of social media
Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the students and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports; A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • To regularly review with the E-Safety Co-ordinator (Faculty Leader) (including e-safety incident logs, filtering / change control logs)
Computing Curriculum Faculty Leader	• To oversee the delivery of the e-safety element of the Computing curriculum
Network Manager/ technician	• To report any e-safety related issues that arise 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 • To ensure that the school's policy on web filtering is applied and updated on a regular basis • To keep 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 • To ensure that the use of the network / Virtual Learning Environment (Learning Platform) / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator (Faculty Leader) or Head Teacher for investigation • 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 • To ensure that all data held on students on the school office machines have appropriate access controls in place

Role	Key Responsibilities
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities where appropriate. • To supervise and guide students carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities). • To ensure that students are fully aware of research skills and 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 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 (Faculty Leader) • 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 students should be on a professional level and only through school based systems, never through personal mechanisms • Log all home communication re. students
Students	• To read, sign and adhere to the Student / Student Acceptable Use Policy (NB: where necessary it would be expected that parents / carers would sign on behalf of the students) • More able students to 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 of and 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 and review of e-safety policies

Role	Key Responsibilities
School Inclusion Officer	• Educating parents and raising awareness as instructed by Head Teacher • Facilitate the Technology Awareness Questionnaire for parents. Publish the findings of the questionnaire for all stakeholders.
Parents/ carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Student Acceptable Use Agreement with their students • To access the school website, Learning Platform and on-line student records in accordance with the relevant school Acceptable Use Agreement • to consult with the school if they have any concerns about their students' use of technology
External groups	• Any external individual or organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication:
The policy will be communicated to staff/students where appropriate/community in the following ways:

- This Policy will be posted on the school website and Learning Platform, and stored on shared drives on the school network;
- This Policy will be part of school induction pack for new staff;
- The school's Acceptable Use agreements will be discussed with students at the start of each year;
- The school's Acceptable Use agreements to be issued to whole school community, usually on entry to the school;
- Signed acceptable use agreements to be held in student 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. Neither the school nor the Local Authority can accept liability for material accessed or any consequences of Internet access.
- Staff and students are given information about infringements in use and possible sanctions. Sanctions include:
    - interview by Head Teacher, Assistant Head Teacher (Pastoral) or E-Safety Coordinator (Faculty Leader);
    - informing parents or carers;
    - removal of Internet or computer access for a period of time;
    - referral to the LA or the police.
- Our E-Safety Co-ordinator (Faculty Leader) and Assistant Head Teacher (Pastoral) act as first points of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school and LA child protection procedures.

Review and Monitoring
The e-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy, Behaviour policy, Personal, Social and Health Education policy and in the School Development Plan.

Version Control

As part of the maintenance involved with ensuring your e-safety policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	Baskerville School E-safety policy
Version	2.0
Date	23/03/2016
Author	e-safety coordinator (Faculty Leader Maths and Computing) e-safety committee
Approved by Head Teacher	Rosemary Adams
Approved by Governing Body	Peter Hogan
Next Review Date	23/03/2017

Modification History			
Version	Date	Description	Revision Author
0.1	12/09/2014	Initial draft	e-safety coordinator (Faculty Leader)

2. Education and Curriculum

Student e-safety curriculum

This school

- has a clear, progressive e-safety education programme as part of the Computing and PSHE curriculum. This covers a range of skills and behaviours appropriate to 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 more able students] 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;
    - 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, or an organisation such as ChildLine or the CLICK CEOP button.
- 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 and will be displayed when a student logs on to the school network;
- 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 students 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 students 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 and on-line gaming / gambling.

Staff and governor training

This school

- Ensures staff are trained on e-safety and qualified to understand what to look out for with regards to any e-safety related issues;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] information and guidance on the e-safeguarding 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;
    - the school newsletters and on the school web site;
    - demonstrations and practical sessions held at school;
    - suggestions for safe internet use at home;
    - provision of information about national support sites for parents.

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 (where necessary it would be expected that parents/carers would sign on behalf of the students);
- 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 and understanding the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students (more able)

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- should provide consent for students 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;
- 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;
- support is actively sought from other agencies as needed (e.g. the local authority and regional BGFL grid, UK Safer Internet Centre helpline) in dealing with e-safety issues;

- monitoring and reporting of e safety incidents takes place and contributes to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's SLT, Governors and the LA;
- 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 students 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:

- Has the educational filtered secure BGFL connectivity through Link2ICT and so connects to the 'private' National Education Network;
- Uses the Link2ICT 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 are 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 that the network is healthy through use of Sophos anti-virus software etc. and that the network set-up so staff and students cannot download executable files;
- Uses LA approved email to send personal data over the Internet or secure remote access were 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 approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes or internet Literacy lessons;
- Has blocked student 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;
- Works in partnership with Link2ICT to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas;
- Ensures all staff and students have signed an acceptable use agreement form and understand that they must report any concerns;
- Ensures students only publish within an appropriately secure environment - the school's learning environment;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age or subject appropriate web sites;
- Plans the curriculum context for internet use to match students' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..;
- Is vigilant when conducting 'raw' image search with students 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 logs or escalates as appropriate to the Technical service provider or Helpdesk 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 students, staff and parents;

- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

This school

- Uses individual log-ins for all users;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Local network auditing software installed;
- Ensures the Systems Administrator is up-to-date with LA services and policies;
- Ensures that storage of all data within the school will conform to the UK data protection requirements;
- Students 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 understand 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 students with an individual network log-in username. They are also expected to use a personal password;
- All students have their own unique username and password which gives them access to the internet, the Learning Platform and their own school approved email account;
- Makes clear that no one should log on as another user and makes clear that students 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 students and one for staff. Staff and students 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 20 minutes and have to re-enter their username and password to re-enter the network];
- Requests that teachers and students 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;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans 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" as defined by HM Revenue & Customs;
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by technical support; equipment installed and checked by approved Suppliers / LA 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;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
  e.g. teachers access their area or the staff shared area for planning documentation via a VPN solution;
- 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 (Management Information Systems) Support, our Head Teacher accessing attendance data on specific students, parents using a secure portal to access information on their child;
- Provides students and staff with access to content and resources through the approved Learning Platform which staff and students 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;
- Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through secure file exchange;
- Follows Link2ICT 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;
- 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.

Password policy

- This school makes it clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find it;
- 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 system;
- We require staff to change their passwords every 90 days.

E-mail

This school

- Provides staff with a Local Authority (LA) email account for their professional use, and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of students or staff on the school website. We use anonymous or group e-mail addresses, for example enquiry@baskvill.bham.sch.uk for communication with the wider public;
- Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law;
- 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 LA-provided 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, link2ICT web filtering monitors and protects our Internet access to the World Wide Web.

Students

- Students are introduced to and use e-mail as part of the ICT/Computing scheme of work;
- Students can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this;
- Students 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 or 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.
- Students 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 only use LA e-mail systems for professional purposes;
- Access in school to external personal e-mail accounts may be blocked;
- Never use email to transfer staff or student personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer);
- 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 Head Teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with the 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 admin@schooladdress. Home information or individual e-mail identities will not be published;
- We do not use students' 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.

Learning platform

- Uploading of information on the schools' Learning Platform is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools Learning Platform will only be accessible by members of the school community;
- In school, students are only able to upload and publish within school approved and closed systems, such as the Learning Platform.

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.
- School staff will ensure that in private use:
    - No reference should be made in social media to students, students' 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 LA;
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

- We have a CCTV policy that we adhere to.

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);
- We ensure staff know who to report any incidents where data protection may have been compromised to;
- All staff are DBS checked and records are held in one central record;
- We ensure ALL the relevant stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed;
  This makes clear staffs' responsibilities with regard to data security, passwords and access;
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of students, to professionals working in the Local Authority or their partners in Students' Services / Family Services, Health, Welfare and Social Services;
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems;
- We ask staff to undertaken 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 20 minutes idle time;
- All servers are in lockable locations and managed by DBS checked staff;
- We have an online back-up service and all mission critical data is backed up daily and all other data is backed up on-sight;
- 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 already have 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 or collected by secure data disposal service;
- We are using secure file deletion software.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Designated 'mobile use free' areas are situated in the setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include: toilets, bathrooms and in some settings - sleep areas and changing areas.
- Mobile phones brought into school are entirely at the staff members', students' and 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.
- Student mobile phones which are brought into school must be turned off or placed on silent and stored out of sight on arrival at school. They must remain turned off or on silent and out of sight during lesson time. Staff members may use their phones during school break times and during lessons/formal times phones should be switched to 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; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head Teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School will contact the police if there is a very strong suspicion that a phone or other handheld device on school site may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent.
- 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.

Students' use of personal devices

- 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 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.
- 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.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting students, 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. 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.
- If members of staff have an educational reason to allow students to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- 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.

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 students in online photographic materials or include the full names of students in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students;
- If specific student 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 student 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;
- Students are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger students as part of their ICT scheme of work;
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, 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.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Index:
Acronyms:
LA – Local Authority
ICT – Information Communication Technology
DBS – Disclosure Barring Service
VPN – Virtual Private Network (In order to access anything from the school network and associated networks this can be done via a VPN)
MIS – Management Information Systems
Link2ICT – Birmingham LA ICT company.