E-SAFETY POLICY

Reviewed:	**September 2013**
Date of Next Review:	**September 2014**

Introduction

This E-safety Policy has been written by the school, building on Birmingham LA policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

Scope

This policy applies to all members of the school community (staff, students, volunteers, parents / carers) who have access to and are users of the school ICT systems, both in and out of 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 school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other E-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the School Governing Body, receiving regular information about E-Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety. The role of the E-Safety Governor will include regular meetings with the E-Safety Coordinator, regular monitoring of E-Safety incident logs and reporting issues including changes in legislation to the full Governing Body.

Head Teacher/Senior Leadership:

The Head Teacher is responsible for ensuring the safety (including E-Safety) of members of the school community, although the day to day responsibility for E-Safety will be delegated to the E-Safety Coordinator, who will report to a designated Senior Leadership Team member, who will ensure that:

- o The E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant
- o There is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles
- o There are regular monitoring reports from the E-Safety Coordinator.
- o The Head Teacher and Senior Leadership Team are fully aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

E-Safety Coordinator:
- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies and related documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- Meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Reports regularly to the Senior Leadership Team/Governors that:
    - the school's ICT infrastructure is secure and is not open to misuse or malicious attack
    - the school meets the E-Safety technical requirements outlined in the Local Authority Security Policies, Acceptable Usage Policy and any other relevant Local Authority or Government E-Safety Policy and guidance
    - users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
    - Link2ICT is informed of any issues arising from the BGfL filtering policy.
    - the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
    - they keep up to date with E-Safety technical information in order to effectively carry out the E-Safety role and to inform and update others as relevant
    - the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the /Head teacher / Senior Leadership for investigation / action / sanction
    - monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

Teaching and Support Staff should ensure that:
- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices.
- They have read and understood the school E-safety Policy
- They report any suspected misuse or problem to the E-Safety Coordinator /Head teacher/Senior Leadership for investigation / action / sanction.
- Digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- Students understand and follow the school E-Safety Policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.

- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Senior Person (DSP):
The DSP should be trained in E-Safety issues and be aware of the potential for serious child protection issues to arise from:
- sharing of Data Protection
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students:
- Are made aware in lessons, form time and by login scripts (via Policy Central) that they should use the school ICT systems in a responsible way to ensure that there is no risk to their safety or the safety of others or the school ICT systems
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:
Parents and carers will be responsible for:
- endorsing the school E-safety policy by reinforcing this with their children
- accessing the school website / VLE / on-line student / student records in accordance with the policy

Community Users
It is school policy not to give access to school ICT systems to visitors or community users of the school.

The International School Internet and Digital E-Safety Policy

Policy Rules

The importance of Internet access
- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet access is an entitlement for those students who show a responsible and mature approach to its use.

Educational benefits of Internet access
- access to world-wide educational resources including museums and art galleries and online libraries;
- inclusion in government initiatives;
- educational and cultural exchanges between students world-wide:
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- staff professional development through access to national developments, educational materials and access to advice on good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA and DFE.

Enhancing learning using the Internet
- The school Internet access will be designed expressly for student / staff use and will include filtering appropriate to category of user.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities particularly through the use of the school VLE and research projects.
- Access levels will be reviewed regularly to reflect the curriculum requirements and age of students.
- Staff will guide students in on-line activities that will support the learning outcomes planned for the students' age, ability and maturity.
- Students at Key Stages 3 and 4 will be educated in the effective use of the Internet in research, including the skills of knowledge search, retrieval and evaluation.

Evaluating Internet content
- The school will ensure that the use of materials derived from the Internet by staff and students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the E-Safety Coordinator in the first instance

Managed E-Mail
- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.
- Access in school to external personal e-mail accounts may be blocked.
- 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.
- Form Tutors will be responsible for monitoring their form groups email usage .
- The forwarding of chain letters is expressly forbidden.

Managing Web site content
- The point of contact on the school Web site will be the school address, school e-mail and telephone number. Staff or students' home information must not be published.
- Web site photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the school Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained and the students approval sought before photographs of students are published on the school Web site.
- The Head teacher or his nominee will take overall editorial responsibility and ensure that content on the school Web site is accurate and appropriate.
- The Web site will comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Using News Groups
- Newsgroups will be made available to students only where an educational requirement for their use has been demonstrated.

Using Chat applications
- Students will not be allowed access to public or unregulated chat rooms.
- Students may only use regulated educational chat environments such as those provided by the VLE. This use will be supervised by teachers and the importance of chat room safety emphasised.
- A risk assessment will be carried out before students are allowed to use any new communication technology in school.

Managing emergent Internet technologies
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school hours. The sending of abusive or inappropriate text messages is forbidden

Authorising and managing Internet access
- The school will keep a record of any students whose parents have specifically requested that internet or e-mail access be denied.
- Students at KS3 and KS4 will be provided with supervised Internet access

Risk assessment
- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head teacher will ensure that the E-Safety policy is implemented and compliance with the policy monitored.

Internet filtering
- The school will work in partnership with parents, the LA, DFE and Link2ICT to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the E-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Filtering strategies will be selected by the school, in concert with Birmingham LA and Link2ICT. The filtering strategy will be selected to suit the age and curriculum requirements of the student.

Introducing the policy to students
- Rules for Internet access will be posted in all rooms where computers are used.
- Students will be informed that Internet use will be monitored.
- Instruction in responsible and safe use will precede Internet access.
- Students will be reminded of the rules and risks at the beginning of any lesson using the Internet
- A course on responsible Internet use will be included on the VLE covering both school and home use.

Staff consultation and responsibilities
- All staff are governed by the terms of the E-safety Policy' in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the E-safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development training and information in safe and responsible Internet use and on the school Internet policy will be provided as required.

ICT System security

- The school ICT systems are reviewed regularly with regard to security.
- Virus protection is installed and updated regularly.
- Security strategies are discussed with Link2ICT, particularly where a wide area network connection is being planned.
- Data Protection sent over the Internet will be encrypted or otherwise secured.
- System utilities and executable files will not be allowed in students' or staff work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The E-Safety Coordinator will ensure that the system has the capacity to take increased traffic caused by Internet use.

Handling complaints

- Responsibility for handling incidents will be delegated to the E-Safety Coordinator in the first instance.
- Any complaint about staff misuse must be referred to the Head teacher.
- Students and parents will be informed of the complaints procedure.
- Parents and students will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact should be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - interview/counselling;
  - 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.

Parental support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus, on the school website and via 'parent workshops'.
- Issues arising out of Internet misuse will be handled sensitively to inform parents without causing undue alarm.
- A partnership approach with parents will be encouraged. This should include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice and access to filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.Interested parents will be referred to organisations such as Child Exploitation and Online Protection (CEOP), ThinkUKnow and Ins@fe.

International School E-Learning Acceptable Use policy

COMPUTING FACILITIES
Users are encouraged to make use of the school's computing facilities for educational purposes. All users are expected to act responsibly , follow procedural guidelines and to show consideration to others.

USE OF TECHNOLOGY
Technology that can be used to store, transmit or manipulate data, such as media rich phones, MP3 players, Personal Digital Assistants (PDAs) and USB media, should be used responsibly and in accordance with the International School Acceptable Use Policy, even when not used with school equipment.

ACCOUNT SECURITY
Users are responsible for the protection of their own network account and should not divulge passwords to anybody. Passwords must be complex; a minimum of eight characters, which must include uppercase and lowercase letters and numbers. Users should not logon to or use any account other than their own and should logoff when leaving a workstation, even for just a short period of time.

USE OF ICT FACILITIES
It is not acceptable to:

- Attempt to download, store or install software to school computers.
- Attempt to introduce a virus or malicious code to the network.
- Attempt to bypass network or system security.
- Attempt to access another user's account.
- Attempt to gain access to an unauthorised area or system.
- Attempt to use any form of hacking/cracking software or system.
- Connect any device to the network that acts as a Wireless Access Point (WAP), bridge or router.
- Connect any device to the network that has access to the Internet via a connection not provided by the school.
- Physically damage or vandalise any computer equipment
- Access, download, create, store or transmit material that is: indecent or obscene, could cause annoyance or offence or anxiety to others, infringes copyright or is unlawful or brings the name of the school in to disrepute.
- Engage in activities that waste technical support time and resources.
- Connect, link or otherwise use on the school ICT network any equipment that is not provided by the school

SECURITY, PRIVACY AND E-SAFETY
- Users are expected to act safely by not publishing personal information online.
- Students may share their interests, ideas, and preference, but must not give out their family name, password, username, email address, home address, school name, city, county or other information that could help someone contact or locate them in person.

- It is not acceptable for anyone to engage in any behaviour that is upsetting or threatening to another user. Any form of online bullying will be dealt with in line with the schools anti-bullying policy.
- Users should not forward private data without permission from the author.
- Users should realise that the school has a right to access personal areas on the network. Privacy will be respected unless there is reason to believe that the Acceptable Use Policy or school guidelines are not being followed.
-

INTERNET ACCESS

- The school's Internet service is filtered to prevent access to inappropriate content and to maintain the integrity of the computer systems. **Users should be aware that the school logs all Internet use.**
- The use of public chat facilities is not permitted unless authorised as part of online learning.
- Users should not attempt to use proxy servers to bypass the school filtering system.
- Users should not copy and use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by examination boards. Information sources should be referenced.
- Users should ensure that they are not breaking copyright restrictions when copying and using material from the Internet.

EMAIL

- Automated software scans all email and removes content that could compromise the integrity of the computer systems or contain unsuitable/offensive content.
- Students are not allowed to use email during lessons, unless the teacher for that lesson has permitted its use.
- If a user receives an email from an unknown person or that is offensive or upsetting, the E-Safety Coordinator should be contacted. Do not delete the email in question until the matter has been investigated.
- Sending or forwarding chain emails is not allowed
- Sending or forwarding emails to a large number of recipients or to 'All Staff' is acceptable only for valid, work related reasons
- Do not open attachments from senders you do not recognise, or that look suspicious.
- Storage and archiving of emails is strictly governed by the amount of memory available in the system; users should follow guidelines issued from time to time on data storage limits
- Users may only use the email facilities provided by the School.

INSTANT MESSAGING/SOCIAL NETWORKING

- The use of Instant Messaging (IM) and Social Networking sites within school is not permitted unless authorised as a part of online learning.
- Students are not allowed to use IM facilities in the VLE during lessons, unless authorised as a part of online learning in that lesson.
- If a user receives a message which is offensive or upsetting, the E-Safety Coordinator must be informed. The message must be kept until the matter has been investigated.
- Never accept files or downloads from people you do not know, or that looks suspicious.

- Do not use a screen-name that is offensive, or gives away additional personal information.
- Do not add unnecessary personal information to your profile or account details.
- In order to stay safe when using public IM or social networking systems (such as MSN, Facebook, MySpace or Bebo) outside school you should additionally:-
    - Only communicate with people on your Contact or Buddy List.
    - Do not accept requests to join your contact list from people you do not already know.
    - Do not add or allow your profile, screen-name or contact information to be shown in online public directories.

BLOGS and WIKIS
- The use of blogs and wikis is allowed.
- Students are not allowed to use Blogs or Wikis in lessons, unless authorised as part of online learning for that lesson
- Users must not share their user name or password or log in as someone else
- Students using blogs are expected to treat blog spaces as classroom spaces. Speech that is inappropriate for class is not appropriate for a blog.
- Users are expected to conduct themselves as representatives of the school. They must not post comments that are defamatory about the school, staff or students.
- If a user receives a message from an unknown person, or which is offensive or upsetting, the E-Safety Coordinator must be informed. The message must be kept until the matter has been investigated.
- Users must respect other user's work and opinions and not maliciously edit any group or individual work. Any user who feels this has taken place should leave the work as it is and contact a relevant member staff.

PRIVATELY OWNED COMPUTERS
Personal laptops and desktops must not be connected to the school network.

International School Password Security Policy

Introduction
The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:
- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- Access to Data Protection is securely controlled in line with the school's data protection policy
- Logs are maintained of access by users and of their actions while users of the system

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

- The management of the password security policy will be the responsibility of the Information Manager
- All users including staff, students, governors and other r community users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report to the E-Safety Coordinator any suspicion or evidence that there has been a breach of security.)
- Passwords for new users and replacement passwords for existing users will be allocated by the school ICT helpdesk. Any changes carried out must be notified to the Information Manager
- Users will change their passwords every 90 days

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. Members of staff will be made aware of the school's password policy:

- At induction
- Through the school E-Safety policy
- Through the Acceptable Use policy

Students and parents will be made aware of the school's password policy:

- in ICT and / or E-safety lessons
- through the Acceptable Use policy

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by E-Safety Coordinator and will be reviewed, at least annually, by the E-Safety Committee.

All users will be provided with a username and password by the ICT helpdesk and a record will be maintained of users and their usernames. .

The following rules apply to the use of passwords:

- Passwords must be changed every 90 days.
- Previously used passwords must not be re-used
- Passwords must be complex; a minimum of eight characters, which must include uppercase and lowercase letters and numbers
- The account will locked following six successive incorrect log-on attempts

- Temporary passwords e.g. those used with new user accounts or when users have forgotten or need to change their passwords, shall be enforced to change immediately upon the next log-on
- Requests for password changes should be directed to the ICT helpdesk to ensure that the new password is only given to the genuine user .

- The "administrator" passwords for the school ICT system, are kept secure and will be made available to the Head teacher or other nominated senior leader if required.

Audi / Monitoring/Reporting/Review

The E-Safety Coordinator will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy
- In the event of a serious security incident, the police may request and if appropriate will be allowed access to any relevant information
- Local authority auditors also have right of access to passwords for audit investigation purposes
- User lists, IDs and other security related information will be given the highest security classification and stored in a secure manner.
- These records will be reviewed by the E-Safety Committee at regular intervals

This policy will be regularly reviewed, at least annually and may be modified in response to changes in guidance and related legislation