E- Safety Policy

BW/LT

July 2015

Principles and purpose

New technologies have become integral to the lives of children and young people in today's society, both within and outside their school lives. The internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and Young people should have an entitlement to safe internet access at all times.

The use of these new technologies can put young people at risk, some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, sharing of personal information
- Risk of being subject to grooming by those with whom they make contact
- The sharing and distribution of personal images without their consent
- Inappropriate communication and contact with others
- Cyber-bullying
- Access to unsuitable video and internet games
- An inability to evaluate the quality, accuracy and relevance of e-information
- Plagiarism and copyright infringement
- Illegal downloading of music and video files
- Excessive use impacting on social and emotional development

Scope of the Policy

This policy applies to all employees and students wherever they may be, both at school or elsewhere such as at home when accessing systems which the school is responsible for.

Roles and Responsibilities

Pupils

It is the responsibility of the students to:

- Keep themselves safe when using ICT
- Report any instances of intentional or non-intentional breaches to this policy

Staff

It is the responsibility of all who work with children within school to:

- Comply with this policy
- Ensure that they understand the risks that the students face
- Promote e-safety at every opportunity with students
- In the event of a disclosure report it to the appropriate Senior Leadership Team in school

E-Safety Coordinator

It is the responsibility of the e-safety coordinator to:

- Develop an eSafety culture
- Act as a named point of contact on all eSafety issues for the Senior Leadership Teams
- Promote the eSafety vision to all stakeholders and supporting them in their understanding of the issues

- Ensure that eSafety is embedded within the continuing professional developments for staff and co-ordinate training as appropriate
- Ensure that eSafety is embedded across the curriculum and activities within the organisation as appropriate
- Ensure that eSafety is promoted to all stakeholders
- Support pastoral teams to decide on appropriate sanctions for pupils
- Monitor and report on eSafety issues to the management team, other agencies and the local authorities eSafety lead as appropriate
- Develop an understanding of the relevant legislation
- Liaise with the local authority and other local bodies as appropriate
- Review and update eSafety policies and procedures on a regular basis

Principal/Head of School

The Principal/Head of School is responsible for:

- Ensuring appropriate arrangements are in place to comply with this policy
- Making sure all users are aware of this policy
- Ensuring that appropriate training is undertaken
- Ensuring that the technical infrastructure / network is as safe and secure as possible
- Updating the list of inappropriate websites which fall through the filtering software
- Supporting the investigation of eSafety incidents
- Applying sanctions to user accounts when necessary

Curriculum

1. All children will be given opportunities to:

    - develop word processing, spreadsheet, presentation and publication skills
    - develop control of wide range of hardware including tablets, laptops and computers.
    - develop an understanding on what ICT peripherals can be used to reach an end goal
    - use a range of multimedia software across the curriculum
    - use ICT to communicate with others
    - simulate and model situations
    - store, retrieve and communicate data effectively
    - use ICT to create music, video and animation
    - research and find out information
    - develop coding and programming skills
    - learn how to be safe online and how to prevent and deal with cyber-bullying
    - learn how to ensure that they work safely on ICT equipment e.g. posture and length of time using a device.
    - incorporate appropriate terminology in their work as well as make good use of ICT learning across the curriculum.
    - manage their own folder directories and file management
    - understand how networks and the world-wide web work
    - develop website building, blogging, wiki and other online skills

2. ICT is integrated across the curriculum, to support outstanding teaching, learning and assessment.

3. All staff and children have access to filtered Internet and the use of e-mail as a key communication tool

4. Children are given opportunities to use a range of technology including tablets, laptops, computers, Interactive whiteboards and screens, externally programmable

devices, cameras, camcorders, audio records, headphones, printing and others peripherals

5. Staff will use ICT to inform and enhance their own professional practise.

6. The use of resources, hardware, and software will be managed, and increasing provision and future development will be planned accordingly.

7. All parents/guardians are required to sign a consent form for ELT and academies to use images of their child(ren).

8. All students are required to complete an Acceptable Use of ICT form. A list of children without consent is kept in each classroom and centrally by the admin team.

Staff Computer Security and Protection

Each member of staff will be provided with personal user account for accessing the computer system, with their own unique username and password. This account will be tailored with permissions to the level of access required and will be for that user's use only. Users must not disclose password information to anyone, including the ICT Technicians, or let other users use the computer systems under their logged on user account. In the event of a password becoming compromised, users will be required to change their password immediately by contacting the ICT Technicians.

- Passwords will be updated as per protocols decided by the Trust's Information Governance Policy.
- Personal computers and devices should not be used for work related purposes.
- Members of staff must not allow a student to have use of a staff account under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, it must be ensured that the computer is either logged off, or locked to prevent anyone using another's account
- USB memory sticks must not be used.
- When publishing, or transmitting non-sensitive material outside of the academy, staff must ensure they follow the appropriate guidance within the Information Guidance Policy
- Academy loaned equipment:
  - Ensure that items of portable computer equipment are stored securely
  - Equipment taken offsite is not insured by the academy. If any academy owned ICT equipment is taken offsite, it should be ensured that adequate insurance cover has been arranged to cover against loss, damage, or theft.
  - Equipment must not be left in cars for any length of time.
  - Ensure additional software is not installed onto any loaned ICT device unless permitted by the Strategic ICT Officer or Principal
  - To keep accurate asset records, portable devices assigned to staff, such as laptops, must be checked and signed for on an annual basis. Failure to comply will result in access to that equipment being revoked.
  - Laptops must be brought to academy every day to ensure that key updates to Anti Virus, Operating System, and school specific software are processed to keep each device up to date and secure.
- Staff must always ensure they are working within the boundaries of the Trust Information Governance Policy.
- All staff are required to sign an Acceptable Use of ICT form annually in order to use the Trust and Academy ICT and systems.

Further guidance around the processes below can be asked of the Trust's eSafety Team that consists of Brett Webster (Strategic ICT Officer), Liz Thompson (Governance Officer) and Jaimie Holbrook (Safeguarding Lead)

Incident Management process in the event of an eSafety incident

Action to be taken when the breach is made by a member of staff:

	Person Responsible
Where there is concern that there has been a breach of the eSafety Policy the person who is made aware of this will report this to the designated lead for eSafety/safe guarding	Member of Staff aware of the incident
The eSafety Co-ordinator will conduct an initial fact finding investigation which will ascertain who was involved, what has occurred. If appropriate the user will be restricted from access to the network	Principal/Head of School
The eSafety Co-ordinator will classify the incident appropriately (high or low severity) and enter details of the incident onto the member of staff's file	Principal/Head of School
The Principal/Head of School/line manager will have been informed and should be given the results of the initial fact finding investigation	Principal/Head of School
If appropriate discussions will take place between the Trust eSafety team and local ICT Technicians to implement any necessary actions e.g. blocking a website	Principal/Head of School
The Principal/Head of School/line manager will discuss the concerns with the Local Authority Designated Officer (LADO) in order to discuss whether there is a need for a Strategy Meeting. During this discussion consideration will be given as to whether the police need to be involved. The Principal/Head of School/line manager will also discuss with Lauren Stones (ELT HR Officer) if the member of staff needs to be suspended or undertake different duties pending the completion of the enquiries.	Principal/Head of School
The Principal/Head of School/line manager will also discuss the incident with the eSafety lead in the Trust as consideration will need to be given to any further actions required.	Principal/Head of School/Line Manager
The strategy meeting process will be completed.	
The designated lead will complete the agencies incident log and send a copy to the Trust's eSafety team	Principal/Head of School

Action to be taken when the breach is made by a pupil:

	Person Responsible
Where there is concern that there has been a breach of the eSafety Policy the adult will make a decision whether to deal with it themselves by applying a sanction and logging it in the relevant systems or report it to the Senior Leadership Team.	Member of Staff aware of the incident
The Senior Leadership Team will conduct an initial fact finding investigation who will ascertain who was involved, what sites have been accessed etc	Senior Leadership Team with support from the Principal/Head of School and ICT support
The Senior Leadership Team will classify the incident appropriately (high or low severity) and enter details of the incident into the relevant system and make a decision about appropriate sanctions, with support from the Trust's eSafety Team if necessary. They will also inform the ICT Technician's to enable them to make changes to the computer system if reduced access is required	Senior Leadership Team with support from Principal/Head of School and ICT support
If necessary, the Principal/Head of School/Head of School will discuss the concerns with the manager of the local authority safeguarding team to establish if there are child protection concerns requiring a Section 47 Child Protection investigation. If this is required the local Safeguarding Team will conduct this investigation as required within the Child Protection Procedures	Principal/Head of School