STEP Academy Trust

Heathfield Academy Trust

E-Safety and Data Security Policy

Date of Policy: **July 2015** **Review: July 2018**

Contents

Appendices

This policy is to be read in conjunction with our Safeguarding Policies and Curriculum Policies:

- *Child Protection; Safeguarding; Anti-Bullying; Behaviour; Behaviour and Exclusion; Health and Safety; Code of Conduct setting out standards and acceptable behaviour for staff; Programming and Computing*
- *Teaching and Learning; Assessment; EYFS; English; Maths; Science, Computing; Arts; PE; RE; MfL SRE and relationships, RRS and Homework.*

STEP Academy Trust

Introduction

ICT in the 21st Century an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Academies need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality.

All users need to be aware of the range of risks associated with the use of these Internet technologies. At Heathfield Academy and across STEP Academy Trust, we understand that we have the responsibility to educate our pupils on e-safety issues, enabling them to remain both safe and legal when using the Internet and related technologies, both inside and outside the classroom.

As an Academy, we hold personal data on learners, staff and other people to help them conduct their day-to-day activities, therefore staff need to be aware of the importance of data security.

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile Internet; technologies provided by the Trust (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto Academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. memory stick, CD Rom) must be checked for any viruses using Academy provided anti-virus software before use

- If your machine is not routinely connected to the Academy network, you must make provision for regular virus updates through your ICT team
- If you suspect there may be a virus on any Academy ICT equipment, stop using the equipment and contact your ICT team immediately via the STEP Web Helpdesk.

Data Security

The accessing and appropriate use of data is something that Heathfield Academy and all STEP Academies take very seriously.

Security

- STEP Academies give relevant staff access to its Management Information System, with a unique ID and password. Level of access is decided by the Headteacher.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing Academy data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.
- Staff keep all Academy related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it should be locked out of sight.
- Data can only be accessed on Academy computers or laptops. Staff are aware that they must not use their personal devices for accessing any Academy data.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- Each Academy maintains a comprehensive inventory of all its ICT equipment including a record of disposal. This full assets list can be found on the STEP Web Helpdesk.

E-Safety

E-Safety - Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the Trust, the Headteachers and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored in their Academy. The named e-safety coordinator in each Academy, usually the Computing Leader, (Tammy Curtis) is responsible for keeping abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

E-S afety in the Curriculum

Computing and online resources are increasingly used across the curriculum. It is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

- We provide opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that maybe encountered outside Heathfield Academy is done informally when opportunities arise and as part of the e-safety curriculum.
- Pupils are aware of the relevant legislation when using the Internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of cyber-bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Safeguard young people online with the view to prevent Radicalisation and Extremism.
- The E-safety Policy is introduced to pupils at the start of every Academy year.
- E-safety posters are displayed prominently within the Academy.

Password security

- All users read and sign an Acceptable Use Agreement to demonstrate they have understood the Trust's E-safety Policy.
- Users are provided with an individual network, email and MLE log in username.
- Pupils are not allowed to deliberately access online materials or files on the Academy network of their peers, teachers or others.
- Staff, governors and children are expected to keep their passwords secret and do not share their passwords with anyone else.
- If staff or children believe their password may have been compromised, they should report it to their line manager / class teacher.

Managing the Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction as well as a potential risk to young and vulnerable people. All use of the London Grid for Learning (LGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected, it will be followed up.

- Students will have supervised access to approved Internet resources through Heathfield Academy's fixed and mobile Internet technology.
- Staff will preview any recommended sites before use.
- If Internet research is set for homework, specific sites will be suggested that have been checked by the class teacher. Parents are advised to re-check these sites and supervise the work.
- All users must observe software copyright at all times. It is illegal to copy or distribute Academy software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Mobile Technologies

- Staff are allowed to bring in personal mobile phones and devices for their own use. Staff should not contact pupils or parents / carers using their personal device.
- Personal mobile devices should not be visible or used during teaching time, and switched off during all Academy meetings.
- Pupils are not permitted to bring mobile devices into Heathfield Academy under any circumstances unless authorised by the Headteachers.
- Heathfield Academy is not responsible for the loss, damage or theft of any personal mobile devices.
- Users bringing personal devices into Heathfield Academy must ensure that there is no inappropriate or illegal content on the device.
- The sending of inappropriate text messages between any members of the academy community is not allowed.

E-Mail

The use of e-mail is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including: direct written contact between Academies on different projects, staff based or pupil based, within school or international. Pupils need to understand how to write an e-mail in relation to their age and good network etiquette; 'netiquette'.

ManagingE-Mail

- Through LGFL, staff have their own e-mail account to use for all Academy business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The Academy email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils or parents using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on Academy headed paper.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account.
- Pupils may only use Academy approved accounts on the Academy system and only under direct teacher supervision for educational purposes.
- Staff must actively manage their e-mail account by:
  - Deleting all e-mails of short-term value;
  - Organising e-mail into folders and carrying out frequent house-keeping on all folders and archives.
- Pupil e-mail users are expected to adhere to the generally accepted rules of netiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive E-mail.
- Staff must inform their line manager if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the Computing curriculum.

Managing other Web 2 technologies

Web 2, if used responsibly both outside and within an educational context, can provide easy to use, collaborative and free facilities. We encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- Students are not permitted to have access to social networking sites on Academy premises.
- All pupils are advised to be cautious about the information given by others on sites, such as users not being who they say they are.
- Pupils are always reminded to avoid giving out personal details on such sites, which may identify them or where they are, for example: full name; address; phone number; Academy details; email address.
- Pupils are advised to set profiles on such networking sites to maximum privacy and to deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Students are asked to report any incidents of cyber-bullying to the Academy.
- Staff may only create blogs, wikis or other web 2 spaces for pupils using the Managed Learning Environment or other systems approved by the Headteachers for example J2E.

Safe Use of Images

Taking of Images and Film

- With the written consent of parents (on behalf of pupils) and staff, appropriate images may be taken by staff and pupils, with Academy equipment.

Consent of Adults Who Work at the Academy

- Permission to use images of all staff who work at the Academy is sought on induction and a copy is located in the personnel file.

Publishing Pupil's Images and Work

On a child's entry into Heathfield Academy, all parents/carers are asked to give permission to use their child's work/photos in the following ways:

- on the Academy or STEP Academy Trust website or Twitter account;
- on the Academy's Learning Platform (Fronter);
- in the Academy prospectus and other printed publications that the Trust may produce for promotional purposes;
- recorded/ transmitted on a video or webcam;

- in display material that may be used in the Academy's communal areas;
- in display material that may be used in external areas, i.e. exhibition promoting the Academy or Trust;
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

The consent form, signed by the parent/carer, is considered valid for the entire period that the child attends this Academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents or custody issues. This information needs to be communicated to the Academy office by the parent/carer. Parents/carers may withdraw permission, in writing, at any time.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to e-safety should be made to the Computing Co-ordinator or Headteachers. Incidents should be logged using the e-safety incident log (see Appendix 5).

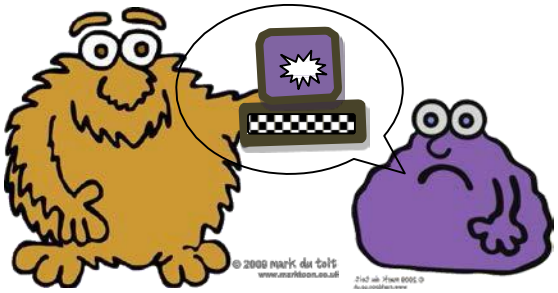
1

Rules for responsible ICT use – KS1

I will only send friendly and polite messages.

I will only use the Internet and email with an adult.

If I see something I don't like on a screen, I will always tell an adult.



I will only click on icons and links when I know they are safe.

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

My teacher has explained what these rules mean.

Rules for responsible ICT use – KS2

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

- I will only use the Academy's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.
- I will not bring files into Academy without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the Academy.
- I will only e-mail people I know, or my teacher 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 have permission or 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 my teacher has given permission.
- 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 my parent, guardian or teacher 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 tell a teacher / responsible adult.

I have read and understood the above rules and I agree that I will keep to them.
Signed:

Appendix

Use of Internet by Pupils

Dear Parent/Carer,

As part of the Government National Grid for Learning Scheme and to support learning opportunities within the Academy, your child/children will, at appropriate times, be given access to the Internet as an information source, a communications tool and a publishing medium.

The Internet is fast becoming a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to support the classroom teacher and the learner is significant and will continue to grow.

There are well publicised concerns regarding access to material on the Internet that would be unsuitable for Academy pupils. Whilst it is impossible to ensure that a pupil will not access such material, at Heathfield Academy we take all reasonable steps to minimise a pupil's access to unsuitable material. These include:

- The use of a filtered Internet Service to prevent access to Internet sites with undesirable material;
- The requirement that, wherever possible, all Internet access during Academy hours will be supervised by a responsible adult;
- The education of pupils as to the potential dangers and legal consequences of accessing certain types of materials.
- Attached to this letter is a copy of the Academy's Policy for Acceptable Computer Use. Also included is a copy of the Academy's Rules for Safe and Responsible Use of ICT and the Internet which we would ask you to read and discuss with your child in a way you feel appropriate to their age and understanding. The Responsible ICT and Internet Use Agreement must be signed by both parent and child before pupils can have access to the Internet.
- We would also ask that you sign the part of the Agreement regarding the publication of work and photographs. Usually, the pictures of children taken at Academy are used for display purposes, but occasionally pictures of children will appear in publications promoting the Academy; these are sometimes available to the general public.
- If you wish to discuss any aspect of the Internet use or photographing the children at Academy, please telephone the office to arrange an appointment.

Yours sincerely,

Headteacher

Responsible ICT and Internet Use Agreement

Pupil's Name: _____

Parent's Consent for Internet Access

I have read Rules for Responsible Use of the Internet and give permission for my son/daughter to access the Internet. I understand that the Academy will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the Academy cannot be held responsible for the nature and content of materials accessed through the Internet other than sites prescribed by the teacher. I agree that the Academy is not liable for any damages arising from the use of the Internet facilities.

Signed: _____

Please print name: _____ Date: _____

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the Academy or STEP Academy Trust website. I also agree that photographs that include my son/daughter may be published subject to the Academy rules that photographs will not clearly identify individuals and that full names will not be used.

Signed: _____

Please print name: _____ Date: _____

Appendix 4

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life in Academy. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Academy e-safety coordinator or the Headteacher.

- I will only use the Academy's email and MLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the Academy or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any Academy business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in Academy, taken off the Academy premises or accessed remotely.
- I will not install any hardware or software without the permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with Academy policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the Academy network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies in Academy can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the Academy approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Academy community ➢ I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in Academy and outside Academy, will not bring my professional role into disrepute.
- I will support and promote the Academy's E-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the Academy.

Signature ……..…… Date ……

Full Name ……..(printed) Job title . . . . . .

Appendix 5

E-Safety Incident Log

Details of ALL e-safety incidents to be recorded by the Computing Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving cyber-bullying may also need to be recorded elsewhere.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Smile and Stay Safe Poster

E-Safety guidelines to be displayed throughout the Academy

and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or Academy. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

13

Appendix 7

Current

Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.legislation.gov.uk/ukpga/1998/29/contents

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.legislation.gov.uk/uksi/2000/2699/contents/made

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to Academy activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.legislation.gov.uk/ukpga/2000/23/contents

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Academies should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information http://www.legislation.gov.uk/ukpga/2003/42/contents

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the

Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain access to computer files or software without permission (for example using another person's password to access files); unauthorised access, as above, in order to commit a further criminal act (such as fraud); impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents

The Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents