



STEP Academy Trust

Online Safety and Social Media Policy

Date of Policy: Autumn 2018

Review: Summer 2020

Contents

Introduction
Computer Viruses
Data Security
Online Safety
Managing the Internet
Social Media and Mobile Technologies
Managing Email
Web 2 Technologies
Safe Use of Images
Misuse and Infringement

Appendices

Appendix 1 – KS1 acceptable use agreement
Appendix 2 – KS2 acceptable use agreement
Appendix 3 – Parent consent forms
Appendix 4 – Governors and staff acceptable use agreement
Appendix 5 – Online safety incident log
Appendix 6 – SMILE poster
Appendix 7 – Current legislation
Appendix 8 – Requirements for creating Social Media sites
Appendix 9 – Social Media site Creation Approval Form

This policy has been agreed by STEP Academy Trust Board of Trustees and applies to all member Academies.

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

- *Safeguarding & Child Protection; Anti-Bullying; Behaviour; Health and Safety; Code of Conduct Setting out Standards and Acceptable Behaviour for Staff;*
- *Teaching and Learning; Assessment; EYFS; Curriculum, SRE and Homework.*

Introduction

ICT in the 21st Century is 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 lifelong 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 sites
- 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 STEP Academy Trust, we understand that we have the responsibility to educate our pupils on Online safety issues, enabling them to remain both safe and legal when using the internet and related technologies, both inside and outside the classroom.

Academies 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, mobile devices, 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, mobile devices and portable media players, etc).

Computer Viruses

- All files downloaded from the internet must be checked for any viruses using Academy provided anti-virus software before use
- If your device 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 ICT Helpdesk.

Data Security

The accessing and appropriate use of data is something that STEP Academies take very seriously and follows the new GDPR guidelines.

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 on Atomwide's USO Password Vault

- Staff are aware of their responsibilities 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.
- USB storage devices are blocked on all academy PCs and laptops.
- Staff should avoid leaving any portable or mobile ICT equipment 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 onsite or via secure remote access as provided. 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 asset list can be found on the STEP Web Helpdesk.

Online Safety

Online Safety - Roles and Responsibilities

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

Online Safety in the Curriculum

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

- The Trust provides opportunities within a range of curriculum areas to teach about Online safety.
- Educating pupils on the dangers of technologies that maybe encountered outside the Academy is done informally when opportunities arise and as part of the Online 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 Online Safety Policy is introduced to pupils at the start of every Academy year
- Online 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 Online Safety Policy.
- Users are provided with an individual network and e-mail 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 to 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.

- Pupils will have supervised access to approved internet resources through the 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.

Social media

The principles set out in this policy are designed to ensure that the use of social media is responsibly undertaken and that confidentiality of pupils and staff and the reputation of individual Academies and the wider Trust are safeguarded.

Social media applies to personal web space such as social networking sites (for example Facebook, Instagram, SnapChat), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopedias such as Wikipedia, and content sharing sites such as Flickr and YouTube.

All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the Academy's Equalities, Child Protection and Safeguarding, and ICT Acceptable Use Policies. In addition, it is important to understand that there is a distinction between use of Academy-sanctioned social media for professional educational purposes, and personal use of social media.

Social media, consent and conduct

Pupils under the age of 13 should not be allowed access to, or be encouraged to create their own personal social media accounts. Children under the age of 13 are not legally allowed to use social media channels such as Facebook and Twitter. However, pupils may be encouraged to observe official Academy social media profiles in an appropriate and safe way, for example, via a feed on the Academy's website;

Any communication received by staff from children on any personal social media sites must be reported to the designated person for Child Protection, the Designated Safeguarding Lead/Officer. In addition, if any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above;

Expected conduct

- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the Academy / Trust and members of its community on any social media accounts;
- Staff should not comment on their Academy, or any other STEP Academy's official social media page from their personal account;
- Staff are also advised to consider the reputation of the Academy / Trust in any posts or comments related to the Academy on any social media accounts;
- Staff should not accept any current pupil of any age or any ex-pupil of the Academy under the age of 18 as a friend, follower, subscriber or similar on any personal social media account, with the exception of relatives;
- Never 'friend' a pupil at the Academy where they are working onto their social networking site;
- Be conscious at all times of the need to keep personal and professional / school lives separate;
- Individuals should not put themselves in a position where there is a conflict between the Academy and their personal interests;
- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the Academy / Trust, or anyone at or connected with the Academy / Trust;
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the Academy's reputation is compromised by inappropriate postings.

Inappropriate and unprofessional

- Users should not engage in activities involving social media which might bring STEP Academy Trust or any STEP Academy into disrepute;
- Users should not represent their personal views as those of STEP Academy Trust or any STEP Academy on any social medium;
- Users should not discuss personal information about other pupils, STEP Academy Trust, any STEP Academy and the wider community they interact with on any social media;

- Users should not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or STEP Academy Trust;
- Staff should not identify themselves as members of STEP Academy Trust or any STEP Academy in their personal web-space, unless specifically linked to an approved job role within the Trust community where it serves a purpose to professionally market their Academy or wider Trust. This is to prevent information being linked with the Academy and to safeguard the privacy of staff members, pupils and parents and the wider school community;
- Pupils should not have contact through any personal social medium with any member of staff. If pupils and members of the wider Academy community wish to communicate with staff they should only do so through official Academy sites created for this purpose;
- Photographs, videos or any other types of image of pupils and their families or images depicting staff members, clothing with Academy logos or images identifying Academy premises should not be published on personal or public web space without prior permission from the Academy;
- We advise that Academy e-mail addresses should not be used for setting up personal social media accounts or to communicate through such media.

Personal use of social media

Under no circumstances should staff make reference to any staff member, pupil, parent or Academy activity / event. The following are also not considered acceptable at STEP Academy Trust:

- The use of the Academy's or STEP Academy Trust's name, logo, or any other published material without written prior permission from the Headteacher or CEO. This applies to any published material including the internet or written documentation;
- The posting of any communication or images which links the Academy to any form of illegal conduct or which may damage the reputation of the Academy. This includes defamatory comments;
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the Academy;
- The Trust accepts that some sites may be used for professional purposes to highlight a personal profile with summarised details, e.g. LinkedIn and Twitter. The Trust would advise that care is taken to maintain an up to date profile and a high level of presentation on such sites if STEP Academy Trust is listed;
- Staff who run blogging/microblogging sites, which have a professional and/or educational status are advised to seek guidance and advice from the head of communications regarding prudence and endorsement of views if there is any link referencing STEP Academy Trust (appendix 8);
- Academy staff should not invite, accept or engage in communications with parents or children from the Academy community in any personal social media whilst in employment at STEP Academy Trust.

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 / Trust meetings.
- Pupils are not permitted to bring mobile devices into our Academies under any circumstances unless authorised by the individual academy (see Individual Academy procedures).
- The Academy is not responsible for the loss, damage or theft of any personal mobile devices.
- Users bringing personal devices into our Academies 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 Academy or international. Pupils need to understand how to write an e-mail in relation to their age and good network etiquette; 'netiquette'.

Managing E-Mail

- Through LGfL/TRUSTnet, staff have their own e-mail account to use for all Academy/Trust 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 e-mail account should be the account that is used for all Academy 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 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 technologies

The Web, if used responsibly both outside and within an educational context, can provide an 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; e-mail 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 spaces for pupils using the Managed Learning Environment or other systems approved by the Headteacher 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 to the Academy, all parents / carers will be 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;
- 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).

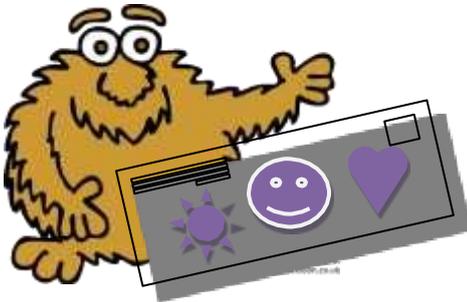
The consent form, signed by the parent / carer, is considered valid for the entire period that the child attends this Academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents or custody issues. This information needs to be communicated to 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 Online safety should be made to the Computing Coordinator or Headteacher. Incidents should be logged using the Online incident log (see Appendix 5).

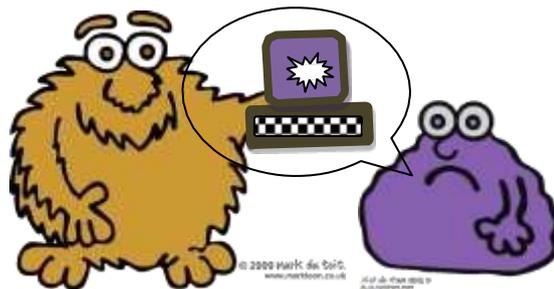
Rules for responsible ICT use - KS1



I will only send friendly and polite messages.

I will only use the internet and e-mail 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 the 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 e-mail 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 3

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 **(Insert Academy name)** 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.
- Under GDPR, we require explicit consent for the use of photos, images, videos, etc. This is outlined in our consent form which we require parents to complete and return.
- 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:

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 school. 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 Online safety coordinator or the Headteacher.

- I will only use the Academy's e-mail 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, following the GDPR regulations and is used appropriately, whether in the Academy, or accessed remotely.
- I will not install any hardware or software without the permission of the ICT team.
- 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 / Trust 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 the 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 the Academy and outside the Academy, will not bring my professional role into disrepute.
- I will support and promote the Academy's Online 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

Online Safety Incident Log

Details of ALL online safety incidents to be recorded by the Computing Coordinator. This incident log will be monitored termly by the Headteacher, Member of EMT 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

Online 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)

Meeeting 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.

E-mails, 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.

Appendix 7

Current Legislation - Acts Relating to Monitoring of Staff e-mail

General Data Protection Regulation (GDPR) May 2018 / Data Protection Act 2018

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

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr>
<http://www.legislation.gov.uk/ukpga/2018/12/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 Online Safety

Racial and Religious Hatred Act 2006

It is 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.

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 their 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 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**General Data Protection Regulation (GDPR) May 2018 / Data Protection Act 2018**

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr>

<http://www.legislation.gov.uk/ukpga/2018/12/contents>

The Freedom of Information Act 2000

www.legislation.gov.uk/ukpga/2000/36/contents

APPENDIX 8

Requirements for creating social media sites on behalf STEP Academy Trust

CREATION OF SITES

- Staff participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of the Academy / Trust.
- Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.
- The proposed audience and level of interactive engagement with the site, for example whether pupils, Academy staff or members of the public will be able to contribute content to the site, must be discussed with the Academy's Headteacher.
- Staff must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.
- Head Teachers must take overall responsibility to ensure that enough resources are provided to keep the site refreshed and relevant. It is important that enough staff are trained and are able to maintain and moderate a site in case of staff absences or turnover.
- There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the Academy's brand and image.
- Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

CHILDREN AND YOUNG PEOPLE

- When creating social media sites for children and young people and communicating with them using such sites, staff must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.
- When creating sites for children and young people, staff must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyberbullying.
- If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.
- Staff must also ensure that the web space they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.

- Care must be taken to ensure that content is suitable for the target age group and contributors or 'friends' to the site are vetted.

APPROVAL FOR CREATION OF OR PARTICIPATION IN WEBSITE

- Social media sites can be created only by or on behalf of the Academy. Site administrators and moderators must be Academy employees or other authorised people.
- Approval for creation of sites for work purposes, whether hosted by the Academy or hosted by a third party such as a social networking site, must be obtained from the Academy's Head Teacher. Approval for participating, on behalf of STEP Academy Trust, on sites created by third parties must be obtained from the Academy's Head Teacher.
- Content contributed to own or third-party hosted sites must be discussed with and approved by the Academy's Head Teacher.
- The Academy's Head Teacher must be consulted about the purpose of the proposed site and its content. In addition, the Head Teacher's approval must be obtained for the use of the Academy logo and brand.
- Staff must complete the Social Media Site Creation Approval Form (Appendix 9) and forward it to the Academy's Head Teacher before site creation.
- Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the Academy's Business Manager/Head Teacher immediately. Staff must not communicate with the media without the advice or approval of the Business Manager/Head Teacher.

CONTENT OF WEBSITE

- Academy hosted sites must have clearly expressed and publicised Terms of Use and House Rules.
- Staff must not disclose information, make commitments or engage in activities on behalf of the Academy's or the STEP Academy Trust without authorisation.
- Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the Academy's or STEP Academy Trust's image, reputation and services.
- Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.
- Academy hosted sites must always include the Academy logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the Academy website.
- Staff must never give out their personal information such as home contact details or personal e-mail addresses on these sites.
- Personal opinions should not be expressed on official sites.

CONTRIBUTORS AND MODERATION OF CONTENT

- Careful consideration must be given to the level of engagement of contributors – for example, whether users will be able to add their own text or comments or upload images.
- The content and postings any STEP Academy Trust hosted site must be moderated. Moderation is the responsibility of the team that sets up or initiates the site.
- The team must designate at least two approved Administrators whose role it is to review and moderate the content, including not posting or removal of comments which breach the Terms of Use. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.
- For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence.
- Individuals wishing to be 'friends' on a site must be checked carefully before they are approved. Their comments must be reviewed regularly and any that do not comply with the House Rules must be removed.

APPENDIX 9

Academy Social Media Site Creation Approval Form

Use of social media on behalf of _____ Academy must be approved prior to setting up sites.

Please complete this form and forward it to the Academy's Headteacher

TEAM DETAILS	
Department	
Name of author of site	
Author's line manager	
PURPOSE	Please describe why you want to set up this site and the content of the site
What are the aims you propose to achieve by setting up this site? What is the propose content of this site?	
PROPOSED AUDIENCES	Who are the proposed audiences of the site? (please tick all that apply)
	<input type="checkbox"/> Pupils of STEP Academy Trust (age range) <input type="checkbox"/> Academy staff <input type="checkbox"/> Pupils' family members <input type="checkbox"/> Pupils from other academies (provide names of Academies) <input type="checkbox"/> External organisations <input type="checkbox"/> Members of the public <input type="checkbox"/> Others; please provide details

PROPOSED CONTRIBUTORS	Who are the proposed contributors to the site? (please tick all that apply)
If contributors include children or adults with learning disabilities, how do you propose to inform and obtain consent of parents or responsible adults?	<input type="checkbox"/> Pupils of the Academy (provide age range) <input type="checkbox"/> Academy staff <input type="checkbox"/> Pupils' family members <input type="checkbox"/> Pupils from other academies (Academy names) <input type="checkbox"/> External organisations
What security measures will you take to prevent unwanted or unsuitable individuals from contributing or becoming 'friends' of the site?	<input type="checkbox"/> Members of the public <input type="checkbox"/> Others; please provide details
ADMINISTRATION OF THE SITE	
Names of Administrators APPROVAL (the site must have at least 2 approved administrators)	Approval from relevant people must be obtained before the site can be created. The relevant managers must read this form and complete the information below before final approval can be given by the Headteacher.
Names of moderators	
Site approval of content of proposed site	Name: Signature: Date:
Who will vet external contributors?	
Proposed date of going live	
Business Manager I approve the aims and content of the proposed site	Name: Signature: Date:
Proposed date for the site and use of Academy brand and logo How do you propose to advertise for external contributors?	
Headteacher	