TEC e-Safety Policy

Adopted and ratified by the Academies Enterprise Trust Board:	
Review Date:	
Accountability: As defined by the AET Governance	AET Board
Responsibility:	AET Board Local Board of Governors

Table of Contents

Executive Summary

The e-Safety policy sets out the framework and expectations that all staff, learners and the academy community should adhere to in respect to the use of computing equipment, the internet and all forms of electronic communication such as email, mobile phones, portals/intranets, social media sites and related learning technologies.
The e-Safety policy is designed to detail the principles all users should adhere to when using these services. This guidance does not attempt to cover every possible situation but should be used as a supporting framework in relation to e-Safety.

1. Introduction

The AET and its academies recognise the benefits and opportunities which new technologies offer to teaching and learning. We provide safe and secure internet access to all learners and staff and encourage the use of ICT and learning technologies in order to enhance skills, promote achievement and enable lifelong learning and world class outcomes.

However, the accessibility and global nature of the internet and associated learning technologies that are available mean that we all need to be aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the academy while supporting staff and learners to identify and manage risks safely, independently and with confidence.

We believe this can be achieved through a combination of security measures, training, guidance and the implementation of the relevant policies. In addition to our duty to safeguard staff and learners and the Every Child Matters agenda, we will do all that we can to make our staff and learners and e-Safe and to satisfy our wider duty of care. The e-Safety policy should be read alongside the following associated AET policies:

AET Academy Staff e-Safety Charter
AET Academy Student e-Safety Charter
AET Academy Corporate Standards in Email Policy
AET Academy Social Networking Policy
AET Data Protection Policies
Human Resources Policies
AET Photograph Policy
AET Academy Website Policy

OfSted Key features of good and outstanding e-Safety practice

From Ofsted's perspective, e-Safety is a critical part of the inspection process. The table below details the key features found when good or outstanding e-Safety practice is in place.

Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of e- Safety issues. High quality leadership and management make e-Safety a priority across all areas of the school (the school may also have achieved a recognised standard, for example the e-Safety Mark). A high priority given to training in e-Safety, extending expertise widely and building internal capacity. The contribution of pupils, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	School-based online reporting processes that are clearly understood by the whole school, allowing the pupils to report issues to nominated staff, for example SHARP. Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.
Staff	All teaching and non-teaching staff receive regular and up-to-date training. At least one staff member has accredited training, for example CEOP, EPICT.
Policies	Rigorous e-Safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors. The e-Safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. The e-Safety policy should incorporate an Acceptable Usage Policy that is signed by pupils and/or parents as well as all staff and respected by
Education	A progressive curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-Safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes.
Infrastructure	Recognised Internet Service Provider or RBC together with age/maturity related filtering that is actively monitored.

Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting e-Safety. Using data effectively to assess the impact of e-Safety practice and how this informs strategy.
Management of Personal Data	The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting e-Safety. Using data effectively to assess the impact of e-Safety practice and how this informs strategy.
Management of Personal Data	The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.

2. Creation, Monitoring and Review

The e-Safety Policy has been prepared with guidance from DfE guidelines on On internet safety previous AET e-Safety Policies and advice and guidance from AET Professional Services and academy colleagues.

It is strongly recommended that an annual review of the e-Safety policy is carried out by a group in the academy that includes the e-Safety officer, the child protection officer (R Walker), senior leadership team representative (T Craig) , a member of the ICT support team (M Khan), learners from the pupil/student council, a teaching staff representative, a support staff representative, a parent representative, a governor representative and a local community police officer.

The impact of this policy will be monitored regularly with a full review being carried out at least once a year. This policy will also be reconsidered where particular concerns are raised or where an e-Safety incident has been recorded.

3. Policy Scope

The e-Safety policy applies to all users, learners, staff and all members of the academy community who have access to the academy ICT systems, both on the premises and remotely. Any user of the academy ICT systems must adhere to and sign a hardcopy of the appropriate ICT Acceptable Use Agreement available on the ICT Policies section of the AET Comms Portal. The e- Safety Policy applies to all use of computing equipment (fixed and mobile), the internet and all forms of electronic communication such as email, mobile phones, portals/intranets

social media web sites.

4. Roles and Responsibilities

There are clear lines of responsibility for e-Safety within the academy. The first point of contact should be [Mrs A Blount], the e-Safety Officer. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager and the e-Safety Officer. All teaching staff are required to adhere to this incident reporting procedure.

When informed about an e-Safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. All learners must know what to do if they have e-Safety concerns and who to talk to. In most cases, this will be the e-Safety Officer or the Child Protection Officer. Where any report of an e-Safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Child Protection Officer may be asked to intervene with appropriate additional support from external agencies.

Listed below are the roles and responsibilities that should be in place in the academy/ are referred to in the e-Safety Policy:

e-Safety Officer

The e-Safety Officer (Mrs A Blount) is responsible for keeping up to date with new technologies and their use, as well as attending any relevant training. She will be expected to lead the e- Safety agenda, review the e-Safety Policy, deliver staff development and training, manage the reporting procedure, record incidents, report any developments and liaise with the AET and external agencies to promote e-Safety within the academy community. He/she may also be required to deliver workshops for parents.

Learners

Learners are responsible for using the academy ICT systems, mobile devices and learning technologies in accordance with the e-Safety Policy, Acceptable User Policy and the AET Academy Student e-Safety Charter which they must sign at the time of registration at the academy. Learners must act safely and responsibly at all times when using the internet and/or mobile/learning technologies. They are responsible for engaging in e-Safety lessons as part of the curriculum and are expected to know and act in line with other relevant academy policies for example; mobile phone use, sharing images, and cyber-bullying. They must follow the reporting procedures where they are worried or concerned, or where they believe an e-Safety incident has taken place involving them or another member of the academy community.

Staff

All staff are responsible for using the academy ICT systems, mobile devices and learning technologies in accordance with the e-Safety Policy and the AET Academy Staff e-Safety Charter which they must sign and submit to the e-Safety Officer/Senior Leader in charge of ICT. S taff must act safely and responsibly at all times when using the internet and/or mobile/learning technologies. Staff are responsible for attending training on e-Safety and displaying a model example to learners at all times through embedded good practice.

All digital communications with learners must be professional at all times and be carried out in line with the AET Academy Corporate Standards in Email Policy. Online communication with learners is restricted to academy provided systems. External platforms not hosted by the academy (for example social media sites) may only be used where a risk assessment has been completed by the member of staff and submitted to the e-Safety Officer and Principal/Headteacher for approval. If approval is granted then the AET Academy Social Networking Policy must be adhered to.

All staff should adhere to the relevant academy policies detailed in the e-Safety Policy and understand the incident reporting procedures. Any incident that is reported to or discovered by **a staff member must be reported to the e-Safety Officer and/or Senior Leader (T Craig Vice Principal) without delay.**

5. Security

The academy will do all that it can to make sure the academy ICT network and systems are safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering (Impero) and firewalls for servers, routers, and all academy provided user devices (desktop/laptop/tablet/mobile etc.) to prevent accidental or malicious access of academy systems and information.

Digital communications, including the academy network, the Google Apps for Education platform, email systems, document storage and academy portals/intranets may be monitored in line with the AET Data Protection Policies.

It is recommended for security purposes that all user account passwords be changed on a 45 - 60 day cycle where practicably possible.

6. Risk Assessment

In making use of new technologies and external online platforms, all staff must first carry out a risk assessment for e-Safety. This consists of a series of questions for the requestor to answer as well as a section in which they can record any relevant comments or evidence. A risk assessment must also be carried out where a learner is learning off site e.g. on work placement. All forms must be submitted to the e-Safety Officer for his/her consideration and approval.

7. Behaviour

Online communication can take many forms, whether it is by email, text, webcam or instant chat. It is essential that all staff and learners are aware of the academy policies that refer to acceptable behaviours when communicating online.

- the academy will ensure that all users of technologies sign and adhere to the standard of behaviours set out in the AET Academy Staff e-Safety Charter and the AET Academy Student e-Safety Charter.

  the academy will not tolerate any abuse of its ICT network, infrastructure or cloud based systems, whether offline or online. All communications by staff and learners should be courteous and respectful at all times as detailed in the AET Academy Corporate Standards in Email Policy.
- any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes. These are available on the Human Resources Policies section of the AET Comms Portal.

Where conduct is found to be unacceptable, the academy will deal with the matter internally. Where conduct is considered to be illegal, the academy will report the matter to the police and other relevant external organisations as required/instructed.

8. Communications

The academy requires all users of ICT to adhere to the appropriate e-Safety charter (AET Academy Staff e-Safety Charter /AET Academy Student e-Safety Charter) which states clearly when email, mobile phones, social media sites, games consoles, chatrooms, video conferencing and web cameras may or may not be used during the academy day. Any required change or extension to these charters will require the permission of the Principal with advice provided by the e-Safety Office..

9. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

All staff and learners should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example.

Academy teaching staff will provide information to learners on the appropriate use of images as detailed in the AET Photograph Policy. This includes photographs of learners and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe. Photographs of activities on the academy premises should be considered carefully and have the correct consent before being published. Approved photographs should not include names of individuals without consent.

10. Personal Information

Personal information is information about a particular living person. The academy collects and stores the personal information of staff and learners regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The academy will keep that information safe and secure and will not pass it onto anyone else without the express consent of the individual or learners' parent/carer as appropriate.

No personal information can be posted to the academy website unless it is in line with the AET Data Protection Policies and the AET Academy Website Policy. Only names and work email addresses of staff will appear on the academy website and no learners personal information will be available on the website without consent and compliance with the AET Data Protection Policies.

Staff must keep learners personal information safe and secure at all times. When using any online or cloud platforms, all personal information must be password protected. No personal information of individuals is permitted off-site unless the member of staff has the written consent from that individual and the written permission of the Principal/Headteacher.

Every user accessing the academy ICT systems and services both onsite or remotely is required to log off on completion of any activity, or where they are physically absent from a device for any period. All academy mobile devices such as a laptops, USB drives, tablets or mobile devices are required to be encrypted, password protected and signed out by the e-Safety Officer or a member of the ICT staff before leaving the premises. Where any personal data is no longer required, it must be securely deleted in line with the AET Data Protection Policies.

11. Education and Training

With the current unlimited nature of internet access, it is impossible for the academy to eliminate all risks for staff and learners. It is our view therefore, that the academy will support staff and learners stay e-Safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For learners

Learners will attend e-Safety lessons with the first of these will taking place at the beginning of each new academic year, with follow up lessons carried out via the curriculum. Issues associated with e-Safety apply across the curriculum and learners will receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies.

Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. A link to the academy e-Safety Policy will be available on the academy network and with the rules highlighted in posters and leaflets around ICT areas and classrooms. Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

For staff

Staff will take part in mandatory e-Safety training at the beginning of each new academic year. This will be led by the e-Safety Officer. Further resources and useful guidance and information

will be issued to all staff following the session. Each member of staff must record the date of the training attended on their CPD calendar/log.

Any new or temporary staff users will receive training on the academy ICT network system and Google Apps for Education platform led by the e-Safety Officer. They will also be asked to sign the AET Academy Staff e-Safety Charter.

12. Incidents and Response

Where an e-Safety incident is reported to the academy this matter will be dealt with very seriously. The academy will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor/teacher or to the academy e-Safety Officer.

Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, the academy will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the AET Academy Staff e-Safety Charter.

Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

13. Feedback and Further Information

The academy welcomes all constructive feedback on this and its linked policies. If you would like further information on e-Safety, or wish to send us comments on our e-Safety Policy, then please contact:

Academy e-Safety Officer:

[Mrs A Blount e safety officer, Head of ICT and Business Studies ablount@tamworthenterprisecollege.org]

or the Academy Principal: Mr S Turney, sturney@tamworthenterprisecollege.org

14. Appendices

14.1 Data Protection

The Data Protection Act 1998 prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to Email in the same way as to other

media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights[1], the Academy respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.

As data controller, the AET/Academy has responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 1998.

In order to comply with its duties under the Human Rights Act 1998, the AET/Academy is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, taking into account the AET / Academy wider business interests. In drawing up and operating this policy the Academy recognises that the need for any monitoring must be reasonable and proportionate.

Auditors (internal or external) are able to monitor the use of the AET/Academy IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data Protection Act 1998, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance[2]. (See Appendix 2)

14.2 Email and Messaging Good Practice Guide

	Good Practice
Read Receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the 'read receipt' option.
Attachment Formats	When attaching a file it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.

[1] 1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[2] Directed Surveillance' is defined as surveillance which is covert (i.e. carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place) but not intrusive, for the purpose of a specific investigation in such a manner as is likely to result in the obtaining of private information about a person.

Email Address Groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of Emails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person's use be sure to indicate people for whom there is some expectation of action or who have central interest. cc to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.
Absent	If you have your own Email address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the 'out of office' message when you are going to be away for some time, e.g. on annual leave. You won't lose your messages, they will await your return, but the sender will know that you're not there and can take alternative action if necessary.
Evidential Record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of Emails could be used in support, or in defence, of the Academy's legal position in the event of a dispute.

Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the Email can result in legally binding contracts being put into place.
Distribution Lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them.
Email threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.
Context	Email in the right context, care should be taken to use Email where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as SHOUTING so consider how the style of your email may be interpreted by its recipient.
Forwarding Emails	Consideration should be given when forwarding Emails that it may contain information that you should consult with the originator before passing to someone else.
Large Emails	For larger Emails, particularly Internet Emails, where possible send at the end of the day as they may cause queues to form and slow other peoples Email.

14.3 Legislative Framework The Human Rights Act1998

This provides for the concept of privacy giving a 'right to respect for private and family life, home and correspondence'. The provision is directly enforceable against public sector employers, and all courts must now interpret existing legislation in relation to the Human Rights Act. Halford v UK 1997 suggests that employees have a reasonable expectation of privacy in the workplace, and employers are recommended to provide workers with some means of making personal communications which are not subject to monitoring, for instance a staff telephone line or a system of sending private Emails which will not be monitored.

Covert monitoring is likely to be unlawful unless undertaken for specific reasons as set out in the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (see below). Employers should make sure workers know of any monitoring or recording of correspondence (which includes Emails, use of Internet, telephone calls, faxes and so on).

14.4 Regulation of Investigatory Powers Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system, and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of communications.

There are two areas where monitoring is not unlawful. These are:

• where the employer reasonably believes that the sender and intended recipient have consented to the interception

• without consent, the employer may monitor in the following circumstances, as set out in the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000. These include:

- to ensure compliance with regulatory practices e.g. Financial Services Authority requirements
- to ensure standards of service are maintained, e.g. in call centres
- to prevent or detect crime
- to protect the communications system this includes unauthorised use and potential viruses
- to determine the relevance of the communication to the employer's business ie picking up relevant messages when someone is away from work.

However, the employer is expected to make all reasonable efforts to ensure system users know that communications may be intercepted, and any such monitoring must also comply with the provisions of the Data Protection Act 1998 (see below), and in particular the Data Protection principles on fair processing.

Data Protection Act

The Information Commissioner - responsible for enforcement of the Data Protection Act - is publishing four codes of practice to help employers comply with the provisions of the data Protection Act. These codes clarify the Act in relation to processing of individual data, and the basis for monitoring and retention of email communications.

The code of practice Monitoring at work: an employer's guide states that any monitoring of emails should only be undertaken where:

- The advantage to the business outweighs the intrusion into the workers' affairs
- Employers carry out an impact assessment of the risk they are trying to avert workers are told they are being monitored

- Information discovered through monitoring is only used for the purpose for which the monitoring was carried out
- The information discovered is kept secure
- Employers are careful when monitoring personal communications such as emails which are clearly personal
- Employers only undertake covert monitoring in the rarest circumstances where it is used for the prevention or detection of crime.

For more information please refer to the AET Data Protection Policies.

14.5 Telecommunications (Lawful Business Practices) (Interception of communications) Regulations 2000

This Act empowered the Secretary of State to make regulations, which allow businesses to intercept communications in the course of lawful business practice and in specific circumstances without the express consent of either the sender or the recipient. Under the Regulations, businesses are required to make all reasonable efforts to inform users of their own systems that such interceptions might take place.

Contract law

It is just as possible to make a legally binding contract via Email as it is by letter or orally. Workers need to be aware of the danger of inadvertently making contracts on behalf of their employer, or varying the terms of any existing contract.

Copyright law

The Copyright, Designs and Patents Act 1988 (as amended) gives the same protection to digital and electronic publications as it does to printed books and other forms of publication. Many websites carry warnings that the information given is copyright and should not be downloaded without agreement from the copyright holder. Similarly copyright exists over software, which should not be downloaded without license.

Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988

These Acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. In the workplace the downloading of certain images from the Internet might subject a worker to charges of criminal behaviour.

Computer Misuse Act 1990

This Act is mainly concerned with the problems of 'hacking' into computer systems.
interception of communications.

There are two areas where monitoring is not unlawful. These are:

• where the employer reasonably believes that the sender and intended recipient have consented to the interception

• without consent, the employer may monitor in the following circumstances, as set out in the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000. These include:

- to ensure compliance with regulatory practices e.g. Financial Services Authority requirements
- to ensure standards of service are maintained, e.g. in call centres
- to prevent or detect crime
- to protect the communications system this includes unauthorised use and potential viruses

- to determine the relevance of the communication to the employer's business ie picking up relevant messages when someone is away from work.

However, the employer is expected to make all reasonable efforts to ensure system users know that communications may be intercepted, and any such monitoring must also comply with the provisions of the Data Protection Act 1998 (see below), and in particular the Data Protection principles on fair processing.

Lawful Business Practice Regulations (LBP)

The LBP Regulations authorise employers to monitor or record communications without consent for a number of purposes, including the following:

- To establish the existence of facts relevant to the business.
- To ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business.
- To ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system.
- To prevent or detect crime.
- To investigate or detect the unauthorised use of telecommunication systems.

The Regulations cover all types of communications including those that are Internet based, by fax and by email.