IT Acceptable Use Policy

Document provenance

This policy was approved by ELT as follows –	
Approver: Executive Leadership Team	Date of Approval: May 2020
Executive Leadership Team (ELT) Chief Operating Officer	Date of Review: May 2022
Unless there are legislative or regulatory changes in the interim, this policy will be reviewed every two years. Should no substantive changes be required at that point, the policy will move to the next review cycle.	

Policy purpose and summary

This policy outlines the obligations on the part of E-ACT staff and other contractors regarding the acceptable use of E-ACT owned ICT devices and the steps the Trust may take to ensure compliance.

Summary of changes at last review:

- E-ACT/academies changed to just E-ACT
- References to related documents inserted into clauses 3.3, 3.4, 9.1
- Data Protection Act 1998 corrected to Data Protection Act 2018
- In clause 1.8 Acts corrected to show full titles
- Clause 6.2 additional wording added in relation to email 'reasonable steps'.

Related policies or guidance:

- Data Protection Policy[1]
- Information Security Policy[2]
- Online Safety Policy[3]
- Social Media Policy[4]
- The Trust's Privacy Notices[5].

[1] https://www.e-act.org.uk/wp-content/uploads/2018/05/Data-Protection-Policy-for-Staff-FINAL.pdf
[2] https://insight.e-act.org.uk/system/files/Information%20Security%20Policy.pdf
[3] https://www.e-act.org.uk/wp-content/uploads/2018/09/Online-Safety-Policy.pdf
[4] https://www.e-act.org.uk/wp-content/uploads/2019/09/Social-Media-Policy.pdf
[5] https://www.e-act.org.uk/privacy-notices/

IT Acceptable Use Policy

1. Introduction and application

1.1. All employees, contractors, consultants, voluntary, temporary and other workers, including all personnel affiliated with third parties who work in both Academy, Regional and National E-ACT teams, must adhere to this policy. It applies when you are working in your usual Academy or office setting and when you are working remotely or travelling.

1.2. For the purposes of this policy 'authorised ICT staff' includes E-ACT's Chief Operating Officer, the Regional Operations Director, National IT Security Manager, Regional IT Lead and Academy ICT staff.

1.3. The purpose of this policy is to recognise the need for you to be able to utilise E-ACT IT systems for the legitimate purposes for which they are intended and for you to carry out your professional duties.

1.4. This policy reflects E-ACT's broad principles in relation to acceptable use of ICT and ICT security. It will be subject to further revision and will be developed so that there will be one suite of documentation relating to e-safety, including individual acceptable use statements signed by you and by pupils/parents.

1.5. You are expected to comply fully with this policy. E-ACT reserves the right to take disciplinary action in the event that it considers that you are acting in contravention of this policy. In addition, and in any event, E-ACT reserves the right to consider legal proceedings against anyone who breaches this policy.

1.6. In the event that you are in any doubt about whether your proposed use of E-ACT IT equipment or systems is in accordance with this policy, then you should seek guidance from your manager, relevant Academy ICT staff, the Regional Operations Director, the National IT Security Manager or E-ACT's Chief Operating Officer before undertaking the activity.

1.7. ICT staff, who are specifically authorised by E-ACT to do so, may monitor and inspect any aspect of use of E-ACT IT equipment/systems, without prior notice, to the extent permitted by law.

1.8. All monitoring, surveillance or investigative activities may be conducted only by authorised ICT staff. This must be done in accordance with the following legislation or regulations:

- The Data Protection Act 2018[6];
- The Human Rights Act 1998[7];
- The Regulation of Investigatory Powers Act 2000 (RIPA)[8] and

[6] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[7] http://www.legislation.gov.uk/ukpga/1998/42/contents
[8] http://www.legislation.gov.uk/ukpga/2000/23/contents

- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000[9].

2. Password security

2.1. Secure and strong passwords are essential to protect the integrity of ICT systems. Passwords should be long, for example, you could use a long lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it is difficult to remember without writing it down. Your password must not be disclosed to anyone else.

2.2. Your password should be difficult to guess, for example, you could base your password on something memorable that no-one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

2.3. You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any Academy account.

2.4. Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

2.5. You must only use your own login and password when logging into ICT systems. Passwords must be changed whenever there is a system prompt to do so or where there is a possibility that there could otherwise be a possible compromise of the system. Passwords should not be re-used or recycled across different systems.

2.6. Where temporary passwords are issued to any individual, for any reason, then they should be changed at first logon to a permanent password.

2.7. Failure to comply with these requirements could lead to you compromising E-ACT system security and would be considered a breach of this policy.

3. Acceptable use of email

3.1. Anyone with a professional E-ACT email has been provided with that email address because it is essential to them being able to carry out their professional duties properly and fully. Professional email accounts are for work related communications and all E-ACT related communications must be conducted via professional email accounts only. E-ACT systems are suitably protected and are the secure and authorised means of conducting work related correspondence.

3.2. All communications made via professional email accounts must relate to professional duties and be of a tone and nature which reflects your professional role and the nature of the

[9] https://www.legislation.gov.uk/uksi/2000/2699/contents/made

communication in question. The degree of care and professionalism should be the same as that applied with a letter being sent out.

3.3. Email is not the preferred form of communication for confidential, personal or other sensitive information (e.g. staff appraisal, any comments relating to job performance or disciplinary issues). Email cannot be regarded as purely private, only to be seen by the receiver. (Please refer to the Information Security Policy).

3.4. All online activity, both in the academy and outside the academy, must not bring the individual, in their professional role or E-ACT into disrepute (Please refer to Social Media Policy for further guidance).

3.5. As detailed in 1.7 and 1.8 above communications via professional email accounts may be monitored from time to time.

3.6. Authorised ICT staff may access your professional email account if you are absent and there is E-ACT related business captured within the account which cannot be otherwise accessed and which requires action before your anticipated return.

3.7. E-ACT recognises that you will be able to access personal email accounts on E-ACT equipment and that it is reasonable for you to be able to do so provided that such access; is limited to before and after your working hours or lunch breaks; is limited to the reading of emails and does not include opening or downloading any attachment received via a personal account without the prior permission of the relevant ICT staff. (This requirement is to protect the integrity of E-ACT systems).

3.8. It is forbidden, at all times, to send files through internal or external email that contain discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libellous, or defamatory content.

4. Acceptable use of internet

4.1. Professional Use

4.1.1. The internet may be used to access relevant websites, including for the purposes of teaching and learning in academies. You are responsible for undertaking a suitable risk assessment and seeking any necessary authorisations related to use of the internet in advance of learning taking place.

4.2. Personal Use

4.2.1. E-ACT recognises that you may need to access the internet for non-work-related purposes from E-ACT equipment, whilst on E-ACT premises or whilst working remotely. As with personal email such access should be limited to before or after your working day or during a lunch break and should be for a reasonable period only. You must not tie up large proportions of internet bandwidth on non-work-related activity, including live

internet feeds; downloading video, images or audio streams; or making repeated attempts to access a locked website.

4.2.2. In any event you may not browse, download, upload or distribute any material that could be considered discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libellous or defamatory.

4.2.3. Personal use of Social Media, personal websites, blogs, etc. should make no reference to E-ACT, its pupils, or colleagues (except in the case of colleagues, with their consent), regardless of whether these sites are accessed while at work or not. Any derogatory comment which expressly or impliedly criticises E-ACT, it's employees, pupils or a relevant third party may be cause for disciplinary action (in addition to any claim for defamation).

5. Acceptable use of ICT equipment and network

5.1. E-ACT ICT Equipment is provided to enable you to fulfil your professional duties.

5.2. E-ACT ICT Equipment may be used to do the following:

- to store E-ACT data;
- run software supplied by E-ACT; and
- load text, images, video or audio in connection with normal working requirements.

5.3. You are responsible for all activity carried out on E-ACT systems, whether accessed via E-ACT ICT equipment or personal equipment. Therefore, you should not allow any unauthorised person to use E-ACT ICT facilities.

5.4. You may not plug personal ICT hardware into E-ACT equipment without specific permission from the relevant member of ICT staff.

5.5. You must not access, load, store, post or send from E-ACT equipment or via a professional email any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to E-ACT or may bring E-ACT into disrepute.

5.6. Use of E-ACT equipment, systems and networks, should be undertaken in compliance with the Data Protection Act 2018, Computer Misuse Act 1990 and the Copyright, Designs and Patents Act 1998. In the event that you have any concerns as to whether the intended use is duly compatible with relevant legislation, then you should seek advice relevant ICT staff prior to undertaking the activity.

6. Viruses

6.1. Viruses can expose E-ACT to very considerable risks.

6.2. You are required to take all reasonable steps to avoid the introduction of any virus on E-ACT equipment, systems or networks.

6.3. Reasonable steps will include, but are not limited to:

- ensuring that files downloaded from the internet, received via email or on removable media such as a memory stick are checked for any viruses using E-ACT provided anti-virus software before being used;
- not using any removable media, such as a memory stick, unless encrypted and with prior approval from authorised ICT Staff;
- be cautious when opening any emails that you are not expecting especially those that contain an attachment;
- do not follow any links to questionnaires, offers, requests, etc. from unknown sources - delete the email;
- do not forward any suspect emails to anybody: Delete it;
- delete emails with attachments that you were not expecting even if you know the person sending, if the wording seems "odd" in some way. These programs can often spoof the Sender field in emails to make it look like someone you know is emailing you;
- not installing any hardware or software without the express permission of the relevant ICT staff;
- allowing any anti-virus software installed on E-ACT ICT equipment to run as it needs to and not interrupting or in any way interfering with such software;
- ensuring that any ICT equipment provided by E-ACT for use off site, benefits from regular E-ACT anti-virus updates either by using it to log onto the relevant networks and allowing the updates to run or by providing it to the relevant ICT staff so that such updates can be undertaken.

6.4. If you suspect there may be a virus on any E-ACT ICT equipment, you must stop using the equipment and contact the relevant ICT staff immediately for further advice.

6.5. Report any attempted phishing e-mail to your Regional IT team in order that they can make sure that investigations can be made into potential other users receiving the email. Often a phishing e-mail is sent to a number of people. See 12.2 below.

7. Landline telephones and mobile phones

7.1. All telephones provided are for work related calls.

7.2. Phone calls of a personal nature should be kept brief and restricted to matters of importance.

7.3. Phone calls to international and premium rate numbers are unacceptable at all times, unless specifically required for your professional duties.

7.4. Mobile telephones should be secured with a suitable PIN or Passcode.

8. Remote access

8.1. As set out in 1.1, remote working and access is covered by this policy in the same way as access on E-ACT equipment at any office or in an Academy.

8.2. It is your responsibility to retain securely all passwords, fobs and any other devices necessary for remote access.

8.3. Particular care must be taken when accessing systems remotely in a public space or private spaces that are shared areas to ensure that screens cannot be viewed by others. You must ensure your actions are compliant with relevant legislation when accessing systems remotely.

9. Safe use of images

9.1. Images of pupils and/or individuals may only be taken, stored and used for professional purposes in accordance with the law and in accordance with E-ACT policies. In any event particular regard must be given to the provision of written consent of the parent, carer or individual to the taking, storage and use of the images (please refer to the Trust's Privacy Notices).

9.2. You are expected to support E-ACT's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the E-ACT community.

10. Personal and confidential data

10.1. All use of personal and confidential data must be in accordance with the Data Protection Act 2018.

10.2. This applies equally, whether in E-ACT premises, taken off the E-ACT premises or accessed remotely.

10.3. You must ensure that personal data is kept secure and is used appropriately.

10.4. In order to protect personal, sensitive, confidential or classified data and prevent unauthorised access to it, this will include, but may not be limited to:

- Ensure screen displays of such data are, at all times, kept out of direct view of any individual who does not need to access that information as part of their professional role and out of direct view of any third parties;
- Ensure screens are locked before moving away from the computer, at any time;
- Ensure logoff from ICT equipment is fully completed when you are going to be away from it for a longer period of time.

10.5. In the event that you consider that you need to take personal data out of E-ACT premises or access it remotely then appropriate authorisation should be sought in advance. Personal or sensitive data taken off site must be encrypted and particular care must be taken when travelling by public transport both to ensure personal data is not inadvertently viewed and to ensure that it is not left behind.

11. E-ACT ICT equipment at home

11.1. You may be supplied with E-ACT equipment to utilise at home and outside of your usual workplace setting. This includes lap-top, tablets, mobile phones and mobile storage devices.

11.2. Such equipment must be treated and used in the same way as it would be in the workplace. You are expected to abide by this policy when using all such E-ACT equipment. This means that you remain liable for the use of the equipment and the passwords for it.

11.3. On request you must make portable and mobile ICT equipment available for anti-virus updates and software installations, patches or upgrades. The installation of any applications or software packages must be authorised by E-ACT, fully licensed and only carried out by E-ACT ICT staff. You must not make copies of any E-ACT software for use outside the organisation or outside the rules prescribed by the particular software's license.

11.4. Data must be saved to the E-ACT network. Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable devices. If it is absolutely necessary to do so then this should be for as short a period as possible and the local drive must be encrypted.

11.5. You are responsible for ensuring that all equipment is stored and kept safely and securely. Any protective equipment must be utilised properly.

11.6. On termination of employment, resignation or transfer, you must return all ICT equipment to your Line Manager. You must also provide details of all of your system logons so that they can be disabled.

11.7. E-ACT will dispose of all redundant ICT equipment in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and the Data Protection Act 2018 (DPA). Any equipment that is to be resold must have a demonstrable audit trail to prove that is has been disposed of in line with ESFA requirements and authorisation has been sought by the same, where appropriate.

11.8. In normal circumstances you should not be using personal equipment for work purposes. Without prejudice to E-ACT's position, in the event that personal equipment is used for work purposes, personal data should not be saved to the local device and when disposing of any such personal device, you are expected to allow E-ACT ICT staff to ensure the hard drive is clear of any work files.

11.9. As detailed above in the section on Personal and Confidential Data, ICT equipment must never be left unattended in an area accessed by the public and/or when travelling. When travelling by car, if you have to leave the car unattended then ICT equipment should be kept locked in the boot and out of sight where it is not possible for you to take the equipment with you.

12. Incident reporting

12.1. You should report any actual security breaches or attempted security breach, loss of equipment or data, to the Data Protection Officer (DPO) – dpo@e-act.org.uk.

12.2. Concerns regarding virus, phishing emails, unsolicited emails, any unauthorised use or suspected misuse of ICT or any of matter of concern, should be reported to your manager and to relevant ICT staff, as a matter of urgency.

12.3. In the event that you receive an email, through your professional email account, either from within E-ACT or from any third party that you consider to be abusive then that should immediately be reported to the relevant Line Manager.

13. Compliance

13.1. All employees are asked to annually declare that they have read, understood, and will comply with E-ACT's IT Acceptable Use Policy as part of their annual staff declaration.