Operational Policy Manual:
E-ACT approval (Audit & Risk Committee): June 2019 (scheduled)
E-ACT LGB ratification: September 2019 (scheduled)

E-ACT

ICT Usage Policy

Operational Policy Manual:
E-ACT approval (Audit & Risk Committee): June 2019 (scheduled)
E-ACT LGB ratification: September 2019 (scheduled)

1. Introduction and Application

All employees, contractors, consultants, voluntary, temporary and other workers, including all personnel affiliated with third parties must adhere to this policy who work in both Academy settings and central E-ACT offices. It applies when you are working in your usual Academy or office setting and when you are working remotely or travelling. An ICT policy for students is contained in Annex A.

For the purposes of this policy 'authorised ICT staff' includes E-ACT's ICT Manager and your Academy's ICT staff.

ICT is an integral part of all business settings and is essential within the context of educational settings. The purpose of the policy is to recognise the need for you to be able to utilise E-ACT/Academy IT systems for the legitimate purposes for which they need it to carry out their professional duties.

This policy reflects E-ACT's broad principles in relation to acceptable use of ICT and ICT security. It will be subject to further revisions 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 students/parents.

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.

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

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

All monitoring, surveillance or investigative activities may be conducted only by authorised ICT staff. You must comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

2. Password security

Secure and strong passwords are essential to protect the integrity of ICT systems. Strong passwords consist of at least 8 characters and include both letters and numbers.

You must always and only use your own logins and passwords when logging into ICT systems. Passwords must be changed whenever there is a system prompt to do so or where there is any possibility that there could otherwise be a possible compromise of the system. If there is no system prompt, passwords must be changed every 56 days as a minimum, more frequent change is recommended.

You should take care to remember your passwords and not to record them anywhere on paper or in an unprotected file. You may only use your own passwords. Passwords are always confidential to you and must never be disclosed to another person.

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

Failure to comply with these requirements can lead to compromise to E-ACT/Academy system security.

3. Acceptable use of email

Anyone with a professional email account (whether in an Academy or whether at head office) 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/Academy related communications must be conducted via professional email accounts only. E-ACT and Academy systems are suitably protected and are the secure and authorised means of conducting work related correspondence.

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

E-mail is not always the most suitable form of communication of confidential, personal or other sensitive information such as staff appraisal, any comments relating to job performance or disciplinary issues. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button.

All online activity, both in school and outside school, must not bring the individual, in their professional role, or E-ACT/Academy into disrepute.

Professional email accounts should not be utilised by you to conduct non work related correspondence.

As detailed above in the Introduction and Application section communications via professional email accounts maybe monitored from time to time.

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

E-ACT recognises that you will be able to access personal email accounts on E-ACT/Academy 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/Academy systems).

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

Professional Use

Use of the internet is essential to you being able to fulfil your professional roles.
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.

Personal Use

E-ACT recognises that you may need to access the internet for non-work related purposes from E-ACT/Academy equipment, whilst on E-ACT/Academy 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 may not tie up large proportions of internet resources on non-work related activity, including live internet feeds; down loading video, images or audio streams; or making repeated attempts to access a locked website.
In any event you may not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Personal use of Social Networking sites, personal websites and blogs, etc. should make no reference to E-ACT/Academy, 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 the E-ACT/Academy, 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

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

E-ACT/Academy ICT Equipment may be used to do the following:

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

You are responsible for all activity carried out on E-ACT/Academy systems carried out under any access/account rights assigned to them, whether accessed via E-ACT/Academy ICT equipment or personal equipment. Therefore, you should not allow any unauthorised person to use E-ACT/Academy ICT facilities and services that have been provided to them.

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

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

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

6. Viruses

Viruses can expose E-ACT/Academy to very considerable risks. You are expected to take all reasonable steps to avoid the introduction of any virus on E-ACT/Academy equipment, systems or networks.

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/Academy provided anti-virus software before being used;

seeking appropriate permissions before plugging any personal equipment into E-ACT/ Academy equipment;

not installing any hardware or software without the express permission of the relevant ICT staff.

allowing any anti-virus software installed on E-ACT/Academy 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/Academy for use off site, benefits from regular E-ACT/Academy 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.

If you suspect there may be a virus on any E-ACT/Academy ICT equipment, you must stop using the equipment and contact their ICT support provider immediately for further advice.

7. Office telephones

Office/Academy landline telephones are provided for work related calls.

Phone calls of a personal nature should be kept brief and restricted to matters of importance. Long personal phone calls are not acceptable.

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

8. Remote access

As set out in the Introduction and Application section above, remote working and access is covered by this policy in the same way as access on E-ACT/Academy equipment at Head office or in Academies.

You are therefore reminded that all passwords, logins and access codes remain personal and confidential and must not be disclosed to anyone else. Particular care needs to be taken to avoid any disclosure of such information in a non-work environment and to ensure you responsibly retain securely all key fobs and other devices necessary for remote access.

Particular care must also always be taken when accessing systems remotely to ensure that screens cannot be viewed other than by the relevant individual. You must ensure their actions are compliant with relevant legislation when accessing systems remotely.

9. Safe use of images

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 any local E-ACT/Academy 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.

You are expected to support the E-ACT/Academy 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 or Academy community.

10. Personal and confidential data

All use of personal and confidential data must be in accordance with the Data Protection Act 1998. This applies equally, whether in E-ACT/Academy premises, taken off the E-ACT/Academy premises or accessed remotely.

You will ensure that personal data is kept secure and is used appropriately. 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;

> Ensuring screen displays of such data are, at all times, be kept out of direct view of any individual who do not need to access that information as part of their professional role and out of direct view of any third parties;
> Ensuring screens are locked before moving away from the computer, at any time;
> Ensuring logoff from the ICT equipment is fully completed when going to be away from it for a longer period of time.
> Ensuring that any print copies made of such data are necessary and that particular care is taken to ensure that printed materials are retained securely and used appropriately.

In the event that you consider that you need to take personal data out of E-ACT/Academy 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/Academy ICT equipment at home

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

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/Academy equipment. This means that you remain liable for their use of the equipment and their passwords for it.

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 the E-ACT/Academy, fully licensed and only carried out by E-ACT/Academy ICT support. You must not make copies of any Academy/E-

ACT software for use outside the organization or outside the rules prescribed by the particular software's license.

Data must be saved to the E-ACT/Academy network. Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. 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.

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

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

E-ACT/Academies will dispose of all redundant ICT equipment in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (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 EFA requirements and authorisation has been sought by the same, where appropriate.

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, when disposing of any such personal device, you are expected to allow E-ACT/Academy ICT staff to ensure the hard drive is clear of any work files.

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.

12. Incident reporting

You should report any actual security breaches or attempted security breach, loss of equipment or data, concerns regarding virus, unsolicited emails, any unauthorised use or suspected misuse of ICT or any of matter of concern, to their manager and to relevant ICT staff, as a matter of urgency.

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.

Appendix A: ICT Acceptable Use Policy

I have read a copy of the ICT Acceptable Use Policy, which I agree to abide by.

I understand any breach of this policy can result in disciplinary action as detailed within the introduction and application of this policy

Signature…………………………………………………………………………………………

Please print Full Name……………………………………………………………………………………….

Location………………………………………………………………………………………

Date…………………………………………………………………………………………