The Active Learning Trust

ICT SECURITY POLICY

This policy is reviewed on an annual basis

History of Document

Issue No	Author/Owner	Date Written	Approved by Trust Board	Comments
1	Director of Finance & Operations / DPO	May 2018	12 July 2018	1st formal issue

1

1.   INTRODUCTION

1.1   ICT enables and enhances the Active Learning Trust's ("Trust") educational and organisational vision and objectives. Information stored on school ICT assets and related systems represents one of the Trust's most valuable assets and must be protected to preserve its confidentiality, integrity and availability in order to enable the Trust's vision and objectives to be achieved.

2.   PURPOSE OF THE POLICY

2.1   The purpose of the ICT Security Policy ("Policy") is to clarify everyone's responsibilities and security measures to be undertaken in accordance with regulatory, legislative and local requirements to ensure that information remains confidential, is protected from unauthorised access or disclosure; is accessible and available and that data integrity is not compromised.

3.   SCOPE

3.1   This Policy is intended for Trust owned ICT equipment and systems when held internally or outside a school/central operations of the Trust. It is intended for anyone who has access to the Trust's administrative and/or curriculum ICT systems or data.

3.2   Privately owned ICT equipment should not be used on a school's network.

3.3   For this Policy definitions are as follows:

- Information covers any method of information creation or collection, including electronic capture and storage, video and audio recordings and any images.

- ICT or ICT system means computing and communications facilities that support teaching, learning and a range of activities in education.

- ICT is the knowledge, skills and understanding needed to employ information and communication technology appropriately.

- ICT equipment means computers, laptops, ipads, tablets, cameras and mobile phones.

- Where the term Headteacher is used this incorporates Executive Headteacher roles where these exist and the Chief Executive Officer of the Active Learning Trust when the statement refers to the central operations of the Trust.

3.4   The Policy incorporates the best practice from within the National Cyber Security Centre's guidance – 10 Steps to Cyber Security in the safe and secure storage of electronic files and data. Such 10 steps are shown in Appendix I.

2

4. RESPONSIBILITY

4.1 The Trust Board has ultimate responsibility for setting this Policy.

4.2 A Headteacher is responsible for ensuring that the requirements relating to this Policy are adopted and adhered to, has overall responsibility for the implementation of the ICT security arrangements in their school, must ensure it is implemented consistently and effectively and is free from discrimination.

4.3 A school's ICT service is responsible for ensuring that security measures are installed on ICT systems and such are monitored for security compliance; advising of any suspected or actual ICT security breaches and ensuring an effective and tested ICT Disaster Recovery Plan is in place.

4.4 Everyone who has access to a school's ICT systems and data must comply with this Policy, the Trust's Email Acceptable Use Policy and its Internet, Social Media and E-Safety Acceptable Use Policy. Anyone outlined in 3.1 above are required to read, accept and agree to abide with all these policies.

4.5 The Trust has produced IT Standards which cover its expected cyber security mechanisms and checks that schools must comply with in order to protect personal data as outlined by the General Data Protection Regulation.

4.6 An Information Management & Cyber Security Governance Group reports to the Trust's Senior Leadership Team and considers Trust wide cyber security and information management matters.

4.7 The Trust's Data Protection Officer and the Trust's Director of Finance and Operations are responsible for monitoring a school's compliance with the Policy; submitting a report on the effectiveness of the Policy (GDPR matters – the Data Protection Officer) and ICT matters (the Director of Finance and Operations) to the Trust Board as a minimum on an annual basis. The Trust's Data Protection Officer is responsible for submitting any reportable security breaches to the Information Commissioner's Office.

5. ICT ASSET ACCOUNTABILITY AND CONTROL

5.1 Procurement

5.1.1 Procurement of ICT equipment and software must be undertaken/co-ordinated by a school's ICT service following appropriate authorisation.

5.1.2 An ICT asset register (however financed) must be maintained by a school's ICT service under whose responsibility the ICT equipment is placed. All items must be accounted for at least annually. In addition a software register must be maintained.

5.1.3 No software which will be used to process personal data should be purchased before a Data Protection Impact Assessment has been undertaken.

5.2   Repairs and Relocation

5.2.1   Users are required to contact a school's ICT service to report any faults or problems that they experience, whether hardware or software related. All faults and problem resolutions must be logged.

5.2.2   Connection, disconnection or relocation of any ICT equipment must be undertaken by or in consultation with a school's ICT service.

5.2.3   Damaged or faulty portable and mobile devices and removeable media must not be used and should be returned to a school's ICT service.

5.3   Disposal/Loss of ICT Equipment

5.3.1   ICT equipment identified for disposal or reuse must be held in secure storage until redeployed or disposed of. Disposal information must be recorded on the ICT asset register.

5.3.2   ICT equipment can either be completely wiped clean of data on a school's premises by a school's ICT service or externally by a Waste Electrical and Electronic Equipment (WEEE) accredited compliant recycling partner, which must provide certificates as evidence of the secure destruction of data.

5.3.3   Any loss of a portable and mobile device and removeable media must be notified immediately to a school's ICT service who will arrange instant disablement of the device (where possible).

5.4   Staff Departure

5.4.1   All staff who leave the employment of the Trust must return Trust owned ICT equipment as part of a school's leavers process. They are also required to confirm that they have deleted any school related emails on their personal mobile phones.

6.   PHYSICAL AND ENVIRONMENTAL SECURITY

6.1   All server, network and communication equipment including associated cabling must be located in secure ICT machine rooms which where possible will be climate controlled. Access to ICT machine rooms must be restricted to authorised persons by keycode locks or swipe card access or similar security devices. Computer rooms must be protected by fire alarms and where possible automated fire extinguishing systems. Eating, drinking and smoking is not permitted in the ICT machine rooms.

7.   EQUIPMENT SECURITY

7.1   Equipment siting and protection

7.1.1   Computer screens, keyboards, printers or other similar devices must be positioned so that information stored or being processed can't be viewed by persons not authorised to such information. ICT equipment must be positioned so it isn't damaged by dust and heat.

7.1.2   With the exception of portable and mobile devices provided specifically for home-working, employees are not permitted to remove ICT equipment from school/Trust premises. Devices must be held securely on and off a school's premises.

7.1.3   All desktop, portable and mobile devices should have a basic input output system (BIOS) passwords and time appropriate automatic screen locking enabled of keyboard or mouse inactivity appropriate for different users in according with the Trust's IT Standards. A user's password will be required to unlock the screen.

7.1.4   Staff must ensure that all desktop, portable and mobile devices are locked prior to leaving them unattended.

7.1.5   Staff who set-up scripts and icons for convenient log ons must not pre-code them with user names or passwords. Generic passwords issued by manufacturers must be changed immediately.

7.1.6   All software media, backups and data should ideally be stored securely in a fire proof safe.

7.2   **Power Supplies**

7.2.1   Critical hardware such as servers and communications equipment should be protected from power supply failure by the use of uninterruptible power supplies (UPS) which offer battery-based backup power.

7.3   **Clock Synchronisation**

7.3.1   In order to ensure the accuracy of any logging or monitoring information, the time clocks on the Trust's servers and ICT devices should be synchronised to a Network Time Protocol (NTP) source.

8.   **ANTI VIRUS SOFTWARE**

8.1   Anti-virus software is installed onto servers and each networked device. Client devices are configured to automatically check and install updates at regular intervals.

8.2   Any Trust owned portable and mobile ICT devices connected to the Internet must be allowed to install automated virus definition and windows security patch updates.

8.3   Non networked ICT equipment e.g. laptops are installed with a standalone copy of anti-virus software which automatically displays a warning message once the virus definition is out of date. Users are required to contact a school's ICT service to arrange regular updates of anti-virus software. Laptops must be connected to the school network at least once every 90 days.

8.4   Any information taken from the Internet will be scanned for viruses by anti-virus software before it is received on a school's local area network.

8.5   Network devices or software designed to capture and/or analyse network traffic must not be installed on school networks without appropriate authorisation from a school's ICT service.

8.6   If personal storage devices (e.g. USB memory sticks) are permitted to be used at a school they must be checked for viruses before data is uploaded to a school network.

8.7   External email messages entering a school network must be automatically checked for malware (computer viruses, trojan horses and worms). Messages containing malware will be retained for up to a month for administrative reasons. The sender of such messages will be informed of the viral content of their email.

8.8   Where a virus is detected this must be reported immediately to a school's ICT service which will attempt to "clean" and rebuild the affected ICT device and update the anti-virus software. The virus scanning software will automatically notify the User of any virus detected.

8.9   Users who install, store or use illegal, unapproved or copied software will be subject to appropriate disciplinary action.

8.10   Firewall protection must be utilised to prevent illegal intrusion via the Internet.

9.   INFORMATION BACK-UP

9.1   Data essential for the day to day running and management of a school should be stored on a school's network server. Back-up copies of data will be taken at regular intervals as determined by the Trust's IT Standard and should be taken before any patch is applied.

9.2   Back-ups should be clearly marked as to what they are and when they were taken. They should be stored away from the system to which they relate in a restricted access fire proof location, preferably off site.

9.3   Instructions for re-installing data or files from back-up should be fully documented and tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

9.4   Data should not be stored on unencrypted portable and mobile devices as these are not included in the automatic nightly back-up of the network servers.

9.5   Copies of data stored on back-ups are deleted in accordance with the Trust's Document Retention Policy.

10.   AUTHORISATION

10.1   Only persons authorised by the Trust's Chief Executive/ Executive Headteacher/ Headteacher are allowed to use a school's ICT systems. The school's ICT service will ensure a User is fully aware of the extent to which they may make use of an ICT system.

11. USER PRIVILEGE MANAGEMENT

11.1 Each system should permit access to a User only on entry of a legitimate unique name (User ID) and password. Users must only use their own unique user name (User ID) and password to access a school network. A standard user profile can be produced for particular grades/staff types. User profiles should be agreed with the Headteacher.

11.2 Only a school's ICT service has administrative privileges on desktop and server systems. ICT Technical staff should have two logins, one Standard User Account and one with Domain Admin privileges which must only be used when necessary.

11.3 A school's ICT service restricts user access e.g. to different parts of systems or to view only, view and update or view, update and delete. It also adds or disables user accounts and sets up/amends user profiles.

11.4 Users must only be supplied with the level of access/least privilege required to perform their work duties and in which they have been trained, throughout a school's network. Users must not attempt to gain access beyond their given access privileges.

11.5 Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

11.6 After entering their unique name (User ID) and password to enter a school ICT system, Users will be reminded of their security responsibilities which they must agree to before being able to enter a school network.

11.7 A school's ICT service should hold a log which records all persons who have been allocated a User account. The log should contain the user name, designation, department, contact details and the user profile. The user profile should provide details of authorised access levels given/ removed and reviews undertaken, together with relevant dates.

11.8 A school's ICT service should undertake a systematic review of User profiles on a regular basis, at least annually, to ensure that current access levels are still appropriate.

11.9 Failed log in attempts will be monitored.

11.10 Personal User IDs must not be shared between people and any group User IDs must not be shared with people outside the approved group of users. All Users will be accountable for any actions undertaken by their personal User ID.

11.11 Access to 'Confidential' and 'Restricted' information will be limited to authorised persons whose role require it, as determined by law, contractual agreement or the Trust's ICT Security Policy.

11.12 Users who have resigned or terminated their contracts or ceased duties must be assessed as to their ongoing need for access to the information systems or facilities. Access can only continue with the permission of the Headteacher. ICT equipment must be returned.

11.13 Users who have been dismissed or subject to disciplinary action or criminal charges which may compromise the security of information systems must not have access to a school's ICT environment, systems or facilities except with the express permission of the Headteacher.

12.   PASSWORDS

12.1 Passwords should be strong and be at least 8 characters long, contain letters, numbers and special characters, include upper and lower-case letters, wholly different from previous passwords used, user rather than system generated and different to the User ID.

12.2 Passwords should be changed once as a minimum every 45 days; enforced password ageing should be implemented to necessitate password changes.

12.3 Users should keep passwords secure and not store them on an ICT device. The "save my password" feature must not be used.

12.4 Users should not disclose passwords to anyone. System administrator passwords are however to be recorded in hard copy by a school's ICT service and kept securely in a safe. These should immediately be changed when a member of a school's ICT service leaves a school.

12.5 If documents are received via email and a password is required to open such documents, the password must not be saved.

12.6 Mobile phones must be accessible only by passwords or a combination of password and facial/finger print recognition.

13.   CRYPTOGRPAHIC CONTROLS

13.1 All staff laptops must have fully encrypted hard drives and personal storage devices e.g. USB memory sticks, where permitted, must be fully encrypted; encryption software must be stored on desktops.

13.2 Where technology prevents the use of encryption (e.g. memory cards used in Digital Cameras) any personal data must not be stored on these devices.

13.3 Emails sent outside the school network (with the exception of the Local Authority/DfE where data is transferred through a secure portal), must be encrypted if personal data is being sent. The de-encryption key must not be sent via the same medium as the encrypted data.

13.4 Encryption is applied to wireless networks, encryption keys should be kept secure and remain the property of the system manger and must not be shared without written permission.

14. OPERATING SYSTEM PATCHING

14.1 Network security vulnerabilities, missing patches and updates will be monitored by a school's ICT service. When it is known that a vulnerability is being actively exploited a patch must be applied immediately.

14.2 Operating systems must be patched up to date with patch releases that are issued from an appropriate manufacturer/supplier within 10 working days.

14.3 If a patch is not available or deployed within the timescale in point 14.2 above, then alternative mitigating action must be taken such as disabling or reducing access to the vulnerable service.

14.4 Where legacy applications are in use that run on unpatchable software, an upgrade plan for these applications must be established.

15. FILTERING OF THE INTERNET

15.1 Access to the Internet should be filtered using an approved system. The effectiveness of such must be monitored by a school's ICT service. Breaches must be reported to a Headteacher and the Trust's Data Protection Officer.

16. EMAIL SECURITY

16.1 The Trust's requirements for use of Emails are covered in its Email Acceptable Use Policy.

17. INTERNET, SOCIAL MEDIA, E- SAFETY SECURITY

17.1 The Trust's requirements for use of the Internet, Social Media and E-Safety are covered in its Internet, Social Media and E-Safety Acceptable Use Policy.

18. REMOTE WORKING/ACCESS

18.1 School data must **NOT** be stored on any portable or mobile ICT device not belonging to a school (including USB memory sticks, cards and hard disks).

18.2 Home working is permitted where authorised by a Headteacher through the use of school owned portable and mobile devices. The installation of any applications or software packages on school owned portable and mobile devices must only be carried out by a school's ICT service.

18.3 All remote access connections must pass through a school's security infrastructure system. Connections which bypass a school's security infrastructure systems (e.g. direct connections to internal modems) are prohibited.

18.4 Access to a school's network and school ICT equipment is not permitted from/allowed to be taken outside the United Kingdom without prior permission from a Headteacher.

18.5   Any documents which are stored on portable and mobile devices must be reviewed regularly by the User and deleted when no longer needed in accordance with the Trust's Document Retention Policy.

19.   ICT SECURITY INCIDENTS

19.1   Each school must have mechanisms in place to properly react and deal with ICT security incidents and violations, both intentional and unintentional and have an effective and tested ICT Disaster Recovery Plan.

19.2   All ICT security weaknesses and incidents, whether suspected or actual, must be reported as outlined in the Trust's Data Protection Policy. Users must not attempt to prove or exploit a suspected ICT security weakness. ICT security incidents include (but are not limited to) for example virus attacks, hardware and software faults, theft or suspected theft of any ICT resources, equipment or information, breach of security resulting in internal fraud or suspected fraud, non-compliance with statutory requirements regarding privacy of information.

20.   ICT SECURITY AWARENESS /TRAINING

20.1   ICT security awareness mechanisms must be in place to ensure anyone who has access to a school's ICT equipment and data are aware of the importance of ICT security, and to properly react and deal with ICT security incidents and weaknesses. User awareness will be supported by regular updates.

21.   MONITORING

21.1   Users should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on Trust owned electronic information and communications systems.

21.2   The Trust reserves the right to monitor, intercept and review, without prior notification or authorisation from Users. Usage of the Trust's IT resources and communications systems, including but not limited to telephone, e-mail, messaging, voicemail, CCTV, internet and social media postings and activities is monitored to ensure that Trust rules are being complied with and for the following purposes:

- to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this Policy;
- to assist in the investigation of alleged wrongful acts; or
- to comply with any legal obligation

21.3   Users consent to monitoring by acknowledgement of the Trust's Code of Conduct and the use of Trust resources and systems. The Trust may store copies of data or communications for a period of time after they are created and may delete such copies from time to time without notice. If necessary, information may be handed to the Police in connection with a criminal investigation.

21.4 Security audit logging is activated on most ICT devices and servers have security audit logging switched on to automatically record events such as failed logon attempts. Critical application systems such as SIMs and PS Financials log, display information and unsuccessful logon attempts.

21.5 All Windows servers event logs are checked during the monthly server maintenance routines. All ICT device alerts are noted during the daily back up procedures.

21.6 The performance of school servers is continually reviewed as part of a regular Server maintenance schedule at each school. This includes a review of system event logs, ICT device messages and disk space.

21.7 Where a CCTV system monitors a school 24 hours a day this data is recorded and may be used as evidence of any alleged wrong doing.

21.8 The Trust reserves the right for appropriate employees to use approved software tools to monitor school network, systems and emails in order to check compliance with this Policy.

21.9 An annual information security/data protection monitoring programme will be undertaken to evidence the effectiveness of this Policy. Evidence will be obtained in order to meet the accountability principle of the General Data Protection Regulation.

22. DISCIPLINARY ACTION

22.1 Disciplinary action may be taken against any User suspected of being in breach of this Policy, including an immediate ban from using a school's ICT facilities.

22.2 Breaches of this Policy may constitute gross misconduct and as such may lead to staff dismissal. For individuals not directly employed by the Trust, breaches of the Policy may result in withdrawal of facilities and referral made to their employer. For all other Users breach of this Policy may be a breach of the Code of Conduct and may lead to sanctions being applied up to and including their removal from the Governing Bodies.

22.3 The Police will be informed where there is a possibility that a criminal offence has been committed.

22.4 If an employee is aggrieved or wishes to register or report a complaint they must follow the Trust's Whistleblowing Policy and/or Staff Grievance Procedures.

23. REPORTING

23.1 The Trust's Director of Finance & Operations is responsible for submitting a report on the effectiveness of this Policy to the Trust Board as a minimum on an annual basis.

24. REVIEW

24.1 This policy will be reviewed on an annual basis by the Trust Board.

APPENDIX I