

IT SECURITY POLICY

Version 4	June 2022
Agreed by SMT	June 2022
Review date	June 2024

- 1. Introduction..... 3
- 2. Scope 3
- 3. Policy Framework..... 4
- 4. Responsibilities 4
- 5. Software Security Measures..... 5
- 6. Anti-Virus Security Measures 6
- 7. Hardware Security Measures 7
- 8. Access and Network Security 8
- 9. Operating System Access Control..... 11
- 10. Data Storage Security 11
- 11. Email and Data Transfers 12
- 12. Reporting IT Security Breaches 12
- 13. Implementation and review 13
- 14. Approval..... 14
- 15. Change history..... 14

1. Introduction

- 1.1 This is a Policy of Age UK East London (“the Company”), registered in England as a private Limited Company by guarantee without share capital use of 'Limited' exemption under No. 07687015 and as Charity No. 1144535 (“the Company”).
- 1.2 This Policy sets out sets out the IT Security measures to be taken by the Company in order to protect its IT and communications devices, infrastructure, computing environment, data and any and all other relevant equipment (collectively, “IT Systems”) from damage and threats whether internal, external, deliberate, or accidental.

2. Scope

- 2.1 This Policy expands on the overall requirement in the Company’s Data Security and Protection Policy that “The Company intends to achieve high standards of data security and protection, particularly in relation to the Processing of Personal Data.”
- 2.2 This Policy also applies to the Company’s Confidential Data and its data in general, whether they are Personal Data or not.
- 2.3 All policies and procedures set out in this document must be followed at all times by the Company, its employees, agents, contractors, volunteers and other parties (“Parties”) acting or working on its behalf in all locations including when working from home.
- 2.4 All IT Systems are to be protected against unauthorised access.
- 2.5 All IT Systems are to be used only in compliance with relevant Company Policies.
- 2.6 All data stored on the IT Systems are to be managed securely and in compliance with Data Protection Law and other relevant UK laws.
- 2.7 All data stored on IT Systems should be classified appropriately, including, but not limited to, Personal Data, Sensitive Personal Data, and Confidential data). All data so classified must be handled appropriately in accordance with its classification.
- 2.8 All data stored on IT Systems shall be available only to those Users with a legitimate need for access.
- 2.9 All data stored on IT Systems shall be protected against unauthorised access and/or processing.
- 2.10 All data stored on IT Systems shall be protected against loss and/or corruption.
- 2.11 All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the Company’s main IT Supplier. Any breach which is either known or suspected to involve Personal Data shall be reported to the Company’s Data Protection Officer.

- 2.12 All Users of the IT Systems must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the IT Supplier. If any such concerns relate in any way to Personal Data, such concerns must also be reported to the Data Protection Officer.

3. Policy Framework

- 3.1 This Policy is part of the Company's Data Security and Protection Policy Framework.
- 3.2 This Policy should be interpreted in conjunction with the Company's primary policy in the Framework, the Data Security and Protection Policy.
- 3.3 Definitions and abbreviations contained in the Company's Data Security and Protection Policy apply equally to this Policy.

4. Responsibilities

- 4.1 The Company's **Senior Information Risk Officer (SIRO)** is responsible for:
- a) the security and integrity of all IT Systems and the data stored thereon;
 - b) ensuring that all IT Systems are assessed and deemed compliant with the Company's security requirements;
 - c) ensuring that IT security standards within the Company are effectively implemented and regularly reviewed, working in consultation with the Company's senior management and Data Protection Officer, as appropriate, and reporting the outcome of such reviews to the Company's senior management;
 - d) ensuring that all Parties are kept aware of the requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the Data Protection Legislation and the Computer Misuse Act 1990.
- 4.2 The Company's **SIRO** and the **Operations & Human Resources Manager** with the support of the **IT Supplier** are responsible for:
- a) assisting all Parties in understanding and complying with this Policy;
 - b) providing all Parties with appropriate support and training in IT security matters and use of IT Systems;
 - c) ensuring that all Parties are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;
 - d) receiving and handling all reports relating to IT security matters and taking appropriate action in response [including, in the event that any reports relate to Personal Data, informing the Data Protection Officer];
 - e) taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;

- f) assisting the SIRO in monitoring all IT security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future; and
 - g) ensuring that regular backups are taken of all data stored within the IT Systems and that such backups are stored at a suitable secure location.
- 4.3 All line managers and supervisors shall be responsible for:
- a) ensuring that all Users under their control and direction adhere to and comply with this Policy at all times.
- 4.4 **IT Suppliers** * are responsible for:
- a) installing, maintaining, servicing, repairing, and upgrading the Company's computer and related systems
 - b) providing advice and guidance on IT matters
- * **Note:** The Company's main IT Supplier is currently **Safetynet IT Ltd**, of Suite A, Unit 10, Century Park, Caspian Road, Altrincham, Cheshire WA14 5HH (the "IT Supplier").
- 4.5 The Company's **Data Protection Office** (DPO) is responsible for:
- a) providing advice and guidance to the Company on interpretation of this Policy
 - b) reviewing this Policy and related procedures regularly to ensure that they comply with current data protection legislation and best practice
- 4.6 **Users of the Company's IT and communications systems** are responsible for:
- a) familiarising themselves with all relevant parts of this and related Policies and comply with them at all times when using the IT Systems.
 - b) using the Company's IT Systems only within the bounds of UK law and must not use the Company's IT Systems for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.
 - c) immediately informing the IT Supplier (and, where such concerns relate to Personal Data, the Data Protection Officer) of any and all security concerns relating to the IT Systems.
 - d) immediately informing the IT Supplier of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.
 - e) Any and all deliberate or negligent breaches of this Policy will be handled as appropriate under the Company's disciplinary procedures.

5. Software Security Measures

- 5.1 All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) will be kept up-to-date and any and all relevant software updates, patches, fixes,

and other intermediate releases will be applied at the sole discretion of the IT Supplier. This provision does not extend to upgrading software to new 'major releases' (e.g. from version 1.0 to version 2.0), only to updates within a particular major release (e.g. from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release, falling within the remit of new software procurement and outside the scope of this provision.

- 5.2 Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied. If the security flaw affects, is likely to affect, or is suspected to affect any Personal Data, the SIRO or the Data Protection Officer shall be informed immediately.
- 5.3 Users may not install software of their own, whether that software is supplied on physical media or downloaded, without the approval of the SIRO. Any software belonging to Users must be approved by the SIRO and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.
- 5.4 All software will be installed onto the IT Systems by the IT Supplier unless an individual User is given written permission to do so by the SIRO. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

6. Anti-Virus Security Measures

- 6.1 Wherever possible, IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall, and other suitable internet security software. All such software will be kept up to date with the latest software patches, updates and definitions.
- 6.2 All IT Systems protected by anti-virus software will be subject to regular full system scans.
- 6.3 All physical media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred. Such virus scans shall be performed automatically upon connection / insertion of media by the User.
- 6.4 Users shall be permitted to transfer files using cloud storage systems only with the approval of the SIRO. All files downloaded from any cloud storage system must be scanned for viruses during the download process.
- 6.5 Any files being sent to third parties outside the Company, whether by email, on physical media, or by other means (e.g. shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate. All email attachments are to be scanned automatically upon sending.

- 6.6 Where any virus is detected by a User this must be reported immediately to the IT Supplier (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Supplier shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or device will be provided to limit disruption to the User.
- 6.7 If any virus or other malware is likely to affect, or is suspected to affect any Personal Data, in addition to the above, the issue must be reported immediately to the Data Protection Officer.
- 6.8 Where any User deliberately introduces any malicious software or virus to the IT Systems this could constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Company's disciplinary procedures.

7. Hardware Security Measures

- 7.1 Wherever practical, IT Systems will be located in rooms which can be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, managers and Users must not allow any unauthorised access to such locations for any reason.
- 7.2 All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) shall be located, wherever possible and practical, in secured, climate-controlled rooms and/or in locked cabinets which may be accessed only by designated members of the IT Supplier.
- 7.3 No Users shall have access to any IT Systems not intended for normal use by Users (including such devices mentioned above) without the express permission of the SIRO. Under normal circumstances, whenever a problem with such IT Systems is identified by a User, that problem must be reported to the IT Supplier. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the SIRO.
- 7.4 All non-mobile devices (including, but not limited to, desktop computers, workstations, and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.
- 7.5 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended, they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts

to avoid such mobile devices from being left unattended at any location other than their private homes or Company premises. If any such mobile device is to be left in a vehicle it must be stored out of sight and, where possible, in a locked compartment.

- 7.6 The IT Supplier shall maintain a complete asset register of all IT Systems. All IT Systems shall be labelled, and the corresponding data shall be kept on the asset register.

8. Access and Network Security

- 8.1 Access privileges for all IT Systems shall be determined on the basis of Users' levels of authority within the Company and the requirements of their job roles. Users shall not be granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.
- 8.2 All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or such other form of secure log-in system as the IT Supplier may deem appropriate and approve. Not all forms of biometric log-in are considered secure. Only those methods approved by the IT Supplier may be used.
- 8.3 All passwords must, where the software, computer, or device allows:
- a) be at least eight (8) characters long;
 - b) contain a combination of alphabetical and numeric characters and where possible upper as well as lower case and special characters;
 - c) be changed at regular intervals;
 - d) be different from the previous password;
 - e) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.); and
 - f) be created by individual Users.
- 8.4 Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone, including managers and the IT Staff. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password, they should change their password immediately and report the suspected breach of security to the IT Supplier and, where Personal Data could be accessed by an unauthorised individual, the Data Protection Officer.
- 8.5 If a User forgets their password, this should be reported to the IT Supplier. The IT Supplier will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.

- 8.6 Users should not write down passwords if it is possible to remember them. If a User cannot remember a password, it should be stored securely (e.g. in a locked drawer or in a secure password database) and under no circumstances should passwords be left on display for others to see (e.g. by attaching a note to a computer display).
- 8.7 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after no more than 5 minutes of inactivity. This time period should not be able to be changed by Users and Users should not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).
- 8.8 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company shall be set to lock, sleep, or similar, after 1 minute of inactivity or less, requiring a password, passcode, biometric or other form of log-in to unlock, wake, or similar. Users may not alter this time period.
- 8.9 Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the SIRO. Any such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared by the SIRO and, where such access renders Personal Data accessible by the outside party, the Data Protection Officer.
- 8.10 Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access.
- 8.11 They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.
- 8.12 Access levels must be agreed by the Company. Each user must be allocated access rights and permissions to computer systems and data that:
 - a) are commensurate with the tasks they are expected to perform
 - b) have a unique login that is not shared with or disclosed to any other user.
 - c) have an associated unique password that is requested at each new login
 - d) User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated.
 - e) System administration accounts must only be provided to users that are required to perform system administration tasks.
- 8.13 User Registration
 - a) A request for access to the organisation's computer systems must first be submitted to the Company's SIRO for non-staff members.

- b) When an employee or other user leaves the organisation, their access to computer systems and data must be suspended at the close of business on their last working day. It is the responsibility of the relevant Director to request the suspension of the access rights via HR, who will notify the Head of Training and Evaluation as appropriate.

8.14 User Responsibilities

- a) It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to the organisations systems by:
 - i) following the Password Policy statements outlined in this policy
 - ii) ensuring that any PC or other device with system access that they are using or responsible for is locked or logged out if it is left unattended
 - iii) leaving nothing on display that may contain access information such as login names and passwords
 - iv) informing HR and the Head of Evaluation and Training of any changes to their role and access requirements
 - v) User must not connect the Company's computers, tablets, mobile phones or other devices to Public Networks, including Wi-Fi networks, unless using an approved Virtual Private Network (VPN) or Mobile Network with the Company's approval.
 - vi) Users must not connect to the Company's networks(s) using their own devices over Public Networks, including Wi-Fi networks, unless using an approved Virtual Private Network (VPN) or Mobile Network with the Company's approval.

8.15 BYOD

- a) Users may connect and use their own ("BYOD") computing and communications devices, including, but not limited to, laptops, tablets, and smartphones, to the Company network(s) and/or use them on behalf of the Company subject to the provisions of all relevant Company Policies, including, but not limited to, this Policy and the **Company's Bringing Your Own Devices to Work Policy**.
- b) Any and all instructions and requirements provided by the IT Supplier governing the use of BYOD devices when connected to the Company network, such as the use of an approved Virtual Private Network (VPN), must be followed at all times.
- c) While BYOD devices are connected to the Company network or to any other part of the IT Systems, the SIRO shall reserve the right to request the immediate disconnection of any such devices without notice.

9. Operating System Access Control

- 9.1 Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section and the Password section above must be applied.
- 9.2 All access to operating systems is via a unique login identity that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).
- 9.3 System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.
- 9.4 Application and Information Access
 - a) Access within software applications must be restricted using the security features built into the individual product. The access must:
 - b) be compliant with the User Access Management section and the Password provisions of this Policy.
 - c) be separated into clearly defined roles.
 - d) give the appropriate level of access required for the role of the user.
 - e) be unable to be overridden (with the administration settings removed or hidden from the user).
 - f) be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
 - g) be logged and auditable.

10. Data Storage Security

- 10.1 All data, and in particular Personal Data and Confidential Data, should be stored securely using passwords and, where practical, data encryption.
- 10.2 All data stored electronically on physical media, and in particular Personal Data and Confidential Data, should be stored securely in a locked box, drawer, cabinet, or similar.
- 10.3 No Personal Data or Confidential Data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is necessary.
- 10.4 No data, and in particular Personal Data and Confidential Data, should be transferred to any computer or device personally belonging to a User unless the User in question is a contractor or sub-contractor working on

behalf of the Company and that User has agreed to comply fully with the Company's Data Security and Protection Policy and the GDPR.

11. Email and Data Transfers

- 11.1 All handling of data for and on behalf of the Company shall be subject to, and must comply with, the provisions of the Company's **Data Security and Protection Policy** at all times. In particular, the following shall apply:
- a) All emails containing Personal Data or Confidential Data must be sent using a secure email system (e.g. NHSmail) or encrypted;
 - b) All emails containing Personal Data or Confidential Data must be marked "confidential";
 - c) Personal Data and or Confidential Data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;
 - d) Personal Data or Confidential Data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
 - e) Personal Data or Confidential Data contained in the body of an email, whether sent or received, should be copied directly from the body of that email, and stored securely. The email itself should be deleted. All temporary files associated therewith should also be securely deleted.
 - f) All Personal Data or Confidential Data to be transferred physically, including that on removable electronic media, shall be transferred in a suitable container marked "confidential".
 - g) Where any confidential or Personal Data or Confidential Data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the User must lock the computer and screen before leaving it.

12. Reporting IT Security Breaches

- 12.1 All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the IT Supplier or the SIRO.
- 12.2 All concerns, questions, suspected breaches, or known breaches that involve Personal Data shall also be referred immediately to the Data Protection Officer who will liaise with the Company's SIRO to handle the matter in accordance with the Company's Data Security and Protection and Personal Data Breach Policies and Procedures.
- 12.3 Upon receiving a question or notification of a breach, the IT Supplier shall, within 24 hours, assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps as it deems necessary to respond to the issue.


- 12.4 Under no circumstances should a User attempt to resolve an IT security breach on their own without first consulting the IT Supplier (or the Data Protection Officer, as appropriate). Users may only attempt to resolve IT security breaches under the instruction of, and with the express permission of, the IT Supplier.
- 12.5 All IT security breaches, whether remedied by the IT Supplier or by a User under the IT Supplier's direction, shall be fully documented.

13. Implementation and Review

- 13.1 This Policy shall be deemed effective as of 27th June 2022. No part of this document shall have retroactive effect and shall thus apply only to matters occurring on or after this date.
- 13.2 This document will be reviewed regularly and normally at least every two years.
- 13.3 This document will be updated as necessary to reflect current best practice, official guidance, and in line with current legislation.
- 13.4 The latest version of this document will be made readily available to all Staff and other relevant parties.

14. Approval

This document has been approved and authorised by:

Name:	Geetha Umaasuthan
Position:	Director of Finance and Operations
Date:	27/6/2022
Due for Review by:	26/06/2024
Signature:	

15. Change History

Version	Section(s)	Issue	Change(s)	Approval	Date
4.0	All	Review	Minor	DPO	24/06/2022
3.0	All	New Data Security and Protection Framework	Multiple		
3.1	8	BYOD	Amended to make clearer provision for the use of BYOD devices I 8.15 and make reference to the new Bringing Your Own Devices to Work Policy.		