Shropshire Telford & Wrekin Age UK

Data Protection, Retention & Security Policy

V10 Updated December 2025

Template Version Control

Version no.	Comment	Date	Author	Next review due
10	Reviewed by DPO July 2025	13/07/2025	Director of Quality & Performance	April 2025
10	Reviewed by CEO and QPD incorporating 6 other policies as appendices	16/12/2025	Director of Quality & Performance	April 2025
10	Sent to PRG	13/01/2025	Director of Quality & Performance	April 2026
10	Noted F&A	03/02/2026	Director of Quality & Performance	April 2026

Contents

1. Introduction to the Data Protection, Retention & Security Policy

This policy applies to all staff, trustees and volunteers of Age UK Shropshire Telford & Wrekin (Age UK STW) and is produced in accordance with the requirements of the Data Protection Act 2018, which implemented the requirements of EU data protection law known as the General Data Protection Regulations (GDPR). These laws came into effect in the UK on 25 May 2018.

Since the UK left the European Union a UK version of GDPR has been introduced, which sits alongside the Data Protection Act 2018; as it will still be essential for UK data protection legislation to remain aligned and compliant with that of the EU.

This policy explains the types of data the organisation may hold, in physical and electronic formats, and how this data must be secured.

The policy also recognises that the majority of personal data is now held electronically and that electronic systems are constantly and rapidly developing. All staff and volunteers are expected to exercise common sense and vigilance in relation to electronic data to ensure it is stored and accessed securely at all times.

All data which relates to any individual must be kept securely and not disclosed to anyone who should not have access to it. However, this policy relates more specificity to the use of personal data as defined by the Data Protection Act.

This policy takes note of the Information Commission Office (ICO) Guidelines for organisations, further information can be found on their website:

https://ico.org.uk/for-organisations/guide-to-data-protection

The purpose of this policy is to enable Age UK STW to:

- Comply with the law in respect of the data it holds about individuals.
- Follow good practice.
- Protect Age UK STW clients, staff, volunteers and other individuals.
- Protect the organisation from the consequences of a breach.
- Define responsibilities.

2. Definitions

Data Subject

The **data subject** is the individual whose **personal data** is being processed. Examples include individuals that are:

- Clients
- Client's relatives / carers / Power of Attorneys
- Employees – current and past
- Volunteers

- Job applicants
- Donors & sponsors
- Staff of suppliers & partner organisations

Personal data means data which relates to a living individual who can be identified:

- From the data.
- From the data and other information which is in the possession of, or is likely to come into the possession of, a data controller or processor.

Personal data examples:

Names, Phone Numbers, E mail Addresses, Postal Address, Passports details, Medical information, Dietary requirements, Images (Photos), IP Addresses, NI No., Financial details, Social information, Location.

It includes any of above which are work related data- Eg. E mail address

Sensitive personal data (Special Category)

Can include someone's physical or mental health or condition, racial or ethnic origin, sexuality, religious or other beliefs, criminal convictions. Sensitive personal data can only be processed under strict conditions; in most cases, this requires getting permission from the person the information is about.

Processing: means the use made of personal data including:

- Obtaining and retrieving.
- Holding and storing.
- Making available within or outside the organisation.
- Printing, sorting, matching, comparing, destroying.

Data Controller

Is the legal 'person', or organisation, that decides why and how personal data is to be processed. The data controller has specific legal responsibilities under the Data Protection Act.

Age UK STW is a **data controller** for the personal data which it collects directly or indirectly about individuals. It is required to be registered with the Information Commissioners Office (ICO) as a data controller under the Data Protection Act 2018.

Data Processor

Is a legal 'person' or organisation processing personal data on behalf of and on the instruction of a data controller.

There should be a written data processing agreement between the data controller and data processor, for the processing to be legal.

Data Protection Officer (DPO)

The appointment of a DPO is legally required for specific data processing activities. The appointed DPO must be independent and hold appropriate qualification and/or experience.

Data Protection Lead

Is the appointed member of the senior management team who is responsible for the implementation and maintenance of data protection legal compliance.

Further information about definitions can be found at the ICO link below:

https://ico.org.uk/for-organisations/guide-to-data-protection

3. Brief Introduction to the Data Protection Act 2018

The Data Protection Act gives individuals the right to know what information is held about them and seeks to promote good practice and protect the individual's right to privacy. It provides a framework to ensure that personal information is handled properly. It applies to organizations holding information about living individuals in electronic or paper format.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection regulations (GDPR) and states that anyone who processes personal information must comply with six key principles, which make sure that personal information is:

Principle a - processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')

The basis of lawful processing must be identified by the data controller

Principle b - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archive purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose ('purpose limitation')

Principle c - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

Principle d - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

Principle e – kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')

Principle f – processed in a manner that ensures appropriate security of the personal data; including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Article 5(2) states that: The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

4. Policy Statement

Age UK Shropshire Telford & Wrekin will:

- Comply with both the legislation and good practice.
- Respect individuals' rights.
- Be open and honest with individuals whose data is held.
- Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently.

Age UK STW recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. Information about staff, volunteers and clients will be used fairly, securely and lawfully, in line with the six principles and not disclosed to any person unlawfully.

The legislation aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account and acted upon. In addition to being open and transparent, Age UK Shropshire Telford & Wrekin will ensure that they comply with the individual rights enshrined in the legislation.

5. Responsibilities

The Data Protection Act 2018 helps make sure that the information held on computers, smartphones, other data storage devices, including portable devices and paper-based systems is managed properly.

The Board of Trustees recognises its overall responsibility for ensuring that Age UK STW complies with its legal obligations.

The board has appointed an external DPO service to support the senior management team with its compliance and registered them as the DPO with the ICO. The DPO will provide periodic assessment of the levels of compliance and provide advice to senior management.

The Chief Executive is the data protection lead for the organisation and has designated duties to the Director of Finance and they each have the following responsibilities:

- Briefing the board on data protection and GDPR responsibilities – Chief Executive.
- Liaising with the appointed DPO – Chief Executive
- Reviewing data protection and related policies – Chief Executive.

- Advising other staff on data protection issues – Chief Executive /Director of Finance.
- Ensuring that data protection induction and training takes place – Chief Executive/line managers.
- Handling subject access requests – DPO/Chief Executive
- Approving unusual or controversial disclosures of personal data – Chief Executive / DPO
- Ensuring contracts with data processors have appropriate data protection clauses – Director of Finance.
- Electronic security – Director of Finance.
- Approving data protection-related statements on publicity materials and letters – Chief Executive.

Every member of staff and all volunteers at Age UK Shropshire Telford & Wrekin who handle personal data will comply with the organisation's policies and operational procedures for handling personal data (including induction and training), to ensure that good data protection practice is established and followed at all times.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work, and to undertake mandatory Data Protection training.

Breaches of this policy will be addressed through Age UK Shropshire Telford & Wrekin's disciplinary procedures.

6. Confidentiality

Confidentiality applies to a much wider range of information than data protection, Age UK STW has a separate Confidentiality Policy which deals with this. The Data Protection Policy should be read in conjunction with Age UK STW's Confidentiality Policy. It can be found here:P:\Organisation & Governance\Policies & Procedures\AUSTW.Policies

Assuring the confidentiality of all personal data being processed is a key requirement of the data protection principles and all persons with access to personal data should be subject to a Confidentiality agreement. It is also both a requirement of our employment contracts and various commercial contracts to which we are obligated legally.

All staff and volunteers will be required to sign their agreement to the requirements of the Confidentiality Policy.

7. Data Subject Rights and Access

Data Subject Rights

The Data Protection Act 2018, strengthened the rights of individuals whose personal data is being held by organisations.

Individuals have the right to:

- Access and obtain a copy of their data on request
- Require the organisation to change incorrect or incomplete data
- Require the organisation to delete or stop processing their data
- Withdraw consent for processing
- Object to the processing of their data
- Transfer their data
- Make complaints to the controller or regulator (ICO)

Special Category Personal Data

The law also specifies that particular types of personal data are categorised as 'Special Category' as they are more sensitive and gives extra protection requirements for them.

AGE UK -STW regularly processes 'Special Category' data and must ensure that its lawful basis for doing this meets the criteria set out in the legislation. All staff and volunteers should be aware that this type of data needs to be handled in a manner that reflects its sensitive nature and maintains confidentiality.

Special Category data includes the following personal data which reveals:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- an individual's health
- a person's sex life or sexual orientation

Personal data which reveals details of criminal convictions or related criminal information, whilst not deemed Special Category; is required to be handled with equal sensitivity / confidentiality and there are also legal requirements addressing this type of data. Staff involved in the processing of criminal check information should ensure awareness of the appropriate handling requirements.

Further information and detail about the principles, data subject rights and data categories can be found on the ICO website:

https://ico.org.uk/for-organisations/guide-to-data-protection

Data Subject Access Requests (DSAR)

Staff and volunteers engaged with any individual for which personal data is held, should ensure that data collected or being collected is accurate and only the data required for the intended purpose is obtained from them.

AGE UK STW shall ensure that its procedures and processes reflect this requirement and the accuracy of personal data held is maintained and not excessive for the purpose of processing or unlawful.

The organisation has implemented a process for ensuring that individuals wishing to exercise their rights to access (Data Subject Access Request -DSAR), is handled efficiently and within the allowed timeframe. (One month)

This process is defined in Appendix 3 of this document (DSAR Procedure).

Staff or volunteers should direct to, or provide any individual wishing to make a request, the dedicated DPO E mail address, which is stated on all Privacy Policies. It is essential that all requests are made formally to the DPO to ensure correct handling and the legitimacy of the request and for individuals to be verified by them.

The DPO will then provide guidance and support to the data protection lead in responding to the request.

The DSAR process should also be the means in which any individual makes a complaint about processing of their personal data.

Data Subject rights are equally applicable to all staff and volunteers as data subjects and as defined on the relevant Privacy policy. Staff or volunteers wishing to exercise their rights can do so through their direct line manager or if preferred the DPO, using the dedicated DPO E mail address.

8. Transparency & Consent

Age UK STW is committed to ensuring that data subjects are informed of our data processing intentions and their rights under legislation.

This will be achieved through the publication and communication of Privacy Policies which provide clients, staff, volunteers, donors and other interested parties the information they need; to make an informed choice as to whether they wish to allow the processing of their personal data.

The data protection lead shall ensure these policies are compliant with legal requirements and made available as appropriate via:

- Website
- Client enrolment processes
- Recruitment processes
- Induction and refresher training
- Internal Network – Policy share drive
- On request by any data subject

All staff and volunteers who are engaged in the enrolment of clients for services, must ensure that the client has been given every opportunity to access the Privacy Policy or have it explained to them; prior to their personal data being collected.

https://www.ageuk.org.uk/shropshireandtelford/privacy-policy/

AGE UK STW uses consent as the basis for lawful processing of personal data in many cases, however; it is policy to ensure transparency of its processing of personal data and allow individuals to make informed decisions about the use of their data.

Where consent is required, it should be given in writing, although for some services it is not always practicable to do so. In these cases, verbal consent will always be sought to the storing and processing of data. In all cases, it will be documented on our database that consent has been given.

Information about clients will only be held, shared or disclosed under the appropriate lawful basis for which it was collected or where there is a legal obligation to do so.

All data subjects will be given the opportunity to opt out of their data being used in particular ways where it is being processed on the basis of their consent (withdrawal of consent); such as direct marketing (see below).

There may be occasions where Age UK STW has a legal obligation to retain data for a certain length of time and in accordance with its Retention policy (Appendix 4). Data retained will be kept to a minimum and should be anonymised wherever possible.

Where consent is required, it shall be formally gained using the controlled consent form applicable to the activity. -

Consent will generally be required for the following activities:

- Capture of equality and diversity information
- Providing Services
- Taking photos or videos
- Direct marketing

The following forms shall be used to record consent:

- Staff Consent & Equal Opportunities Form
- Volunteer Consent & Equal Opportunities Form
- Client Consent Form
- Photo / Video Consent Form

9. Direct Marketing

Data Protection legislation requires that individuals are not subject to any direct marketing, without their expressed consent.

Age UK STW will treat the following unsolicited direct communication with individuals as marketing:

- Seeking donations and other financial support.
- Promoting Age UK STW events direct to clients.
- Promoting membership to supporters.
- Promoting sponsored events and other fundraising exercises.

- Marketing on behalf of any other external company or voluntary organisation.
- Any of the above included in correspondence which is not marketing related.

It is AGE UK STW policy that all Marketing calls, E mail or text messages can only be sent to individuals who have expressly consented to receiving them and this consent has been recorded.

All marketing which is sent out to consenting individuals shall provide the option to withdraw consent for marketing (Opt out) or specific ways in which it's received.

On receipt of such requests, the individual must be removed from all marketing lists or their preferences updated.

Staff should not use previous engagement with an individual as a legitimate basis on which to send marketing information. Marketing lists / consent must be verified prior to each marketing campaign.

Telephone and Mailing Preference Service

Any marketing campaign by phone or post, must also confirm that the individuals are not registered with the Telephone or Mailing preferences services.

Age UK Shropshire Telford & Wrekin is registered with the Fundraising Preference Service and the Age UK Data Suppressions list which regularly updates us on those who do not wish to be contacted.

10. Limitation of Personal Data

The Data Protection Act and principles require that personal data collected is the minimum required to achieve the purpose for which it is collected. Staff and Volunteers should ensure that whilst engaging with our clients only the information that AGE UK STW requires is to provide it's services and support; is sought, stored or recorded.

Additional personal information which clients may reveal voluntarily during engagement with them, may not be used or disclosed to others; unless it is considered to be in the interest of their welfare or safety and only after consultation with the Data Protection Lead.

AGE UK STW will ensure that the controlled documents which it provides for the purposes of collecting personal information, are formatted in such a way that there is limitation to what is collected.

Personal information which has been collected and held in storage in either hard copy or electronic format, can only be retained for the period of time for which it is assessed by AGE UK STW as needed and/or for the time it is legally required to be held. It is essential that Staff and Volunteers maintain their records with this principle in mind. Personal data which is held electronically, is secure and backed up regularly; which should in many cases mean that hard copies of the same data are not required to be kept.

The secure storage, length or period of retention and methods of deletion, of both paper and electronic data are defined in the organisations record retention procedures provided as Appendix 4, which should be read alongside this policy.

11. Technical & Organisational Measures

The Data Protection Act requires that AGE UK STW take adequate Technical and Organisational measures to maintain the integrity and confidentiality of personal data for which it is responsible. These measures should be appropriate to the types of data processing that we conduct and based on the risks of that processing. AGE UK STW has therefore assessed such risks and implemented measures accordingly, to ensure that its working methods and processing systems provide security through design.

The Data Security Policy Appendix 1 , is provided to Staff and Volunteers in order that they are aware of both Technical and Organisational measures relevant to them in maintaining personal data security.

Staff and Volunteers are also required to read and understand the AGE UK STW policy on the acceptable use of IT communications and social media Appendix 2

12. Information Incident Management / Non-Conformance / Data Breach

A data security incident is any event which has or had potential to cause the loss, unauthorised access or release of personal or commercial data, for which AGE UK STW is responsible.

Personal data is as defined by the Data Protection Act 2018:

> **"any information relating to an identified or identifiable living individual"**

A data breach is as defined by the Data Protection Act 2018:

> **"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"**

All staff and volunteers are mandatorily required to report immediately actual, suspected or potential data breaches or security incidents to the DP Lead. There are legal requirements for the reporting to the ICO of qualifying personal data breaches within 72Hrs of discovery; it is therefore important that the process of investigation is not delayed.

The DP Lead in liaison with the relevant senior managers and DPO, will in accordance with the Data Breach Procedure Appendix 5; be responsible for the investigation and handling of any such incidents.

Staff and volunteers should not discuss any knowledge they have of an actual or suspected data breach or security incident; with anyone else within the organisation or external to it. It is vital that a full investigation is first conducted to assess the validity and impact of reported incidents; prior to any communication of the event taking place. Inaccurate or inflated reports of incidents have the potential to cause AGE UK STW reputational damage and a loss of customer confidence. Communication regarding any incident will be handled by the DP Lead and/or DPO to the relevant interested parties.

Staff or volunteers receiving enquiries from customers or other external parties (including the media), should not make any comment and direct those enquiring to the DP Lead.

Staff should also be aware of AGE UK STW Press & Media Contact procedure: -

P:\Organisation & Governance\Policies & Procedures\AUSTW.Policies

13. Staff Training and Acceptance of Responsibilities

All staff and volunteers who have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process, including the Data Protection & Security Policy, , Confidentiality Policy and the operational procedures for handling personal data. All staff will be expected to adhere to all these policies and procedures at all times.

All staff and volunteers will undertake the Bigger Picture induction training which include a section on data protection. Age UK Shropshire Telford & Wrekin will provide opportunities for staff to explore data protection issues through training, team meetings and supervisions. We also provide on-line mandatory training for all staff on data protection, which all staff must undertake on a regular basis.

APPENDIX 1 – DATA PROTECTION & SECURITY POLICY

A1.1 Introduction & Scope

This appendix to our policy sets out AGE UK STW requirements for the implementation of Data Security Policy across all processing activities and compliance with these requirements is mandatory on all staff and volunteers. The measures outlined in this appendix to our policy also include the measures to be applied by Staff or Volunteers working at home (Remote Working).

A1.2 Responsibilities

The Data Protection Lead and Senior Management Team are responsible overall for all aspects data security and shall ensure that adequate risk assessment of data processing activities has been undertaken.

AGE UK STW shall have an appointed Data Protection Officer (DPO), who will liaise with and advise the DP Lead.

The senior management team are responsible for the development, implementation and monitoring of effective risk-based data security controls; which align with policies and all statutory and regulatory requirements.

All staff and volunteers have a responsibility for the protection of data being processed by the business, adherence with all implemented data security controls and to notify senior management if they have concerns about any aspect of data security.

All staff shall be required to read the organisations confidentiality policy and sign to say they have done so.

The Data Protection Act 2018 places a legal responsibility on the business and individuals to ensure that the integrity and confidentiality of any personal data being processed is maintained.

The regulatory body in the UK for data protection is the Information Commissionaires Office (ICO), who will prosecute both businesses and individuals for any breaches of data protection legislation; which can potentially result in very large fines and/or a criminal record.

The security of client provided data can also be a contractually mandatory requirement, therefore the loss or compromise of this data will equally result in negative impact for the business and its employees.

The security of Personal Data has rapidly become one of the most likely risks having substantial impact on businesses; without the diligence of all staff and volunteers involved in its processing the potential for a data breach is significant.

A1.3 Organisational Measures

Risk Management

The DP Lead shall ensure that the risks to Data Assets are understood and appropriate Organisational and Technical measures are identified for implementation to manage identified risks. Risk Assessment shall:

- Identify all Data Assets for which it has responsibility or influence and the intended means of processing those assets.

- Identify applicable statutory, regulatory or contractual requirements with relevance to identified Data Assets.
- Identify those assets which also have value to the business in assuring the security of Data Assets and would impact security if unavailable or compromised.
- Conduct assessment of threats to and vulnerabilities of identified Data and Business Assets.
- Assess the risks associated with the intended processing of identified Data Assets, with reference to identified threats, vulnerabilities and current security measures of all Data and Business assets.
- Determine the acceptability of identified risks and/or determine appropriate measures to treat those risks which are not acceptable; prior to commencement of processing.
- Regularly review risk assessments with reference to evolving threats / vulnerabilities, process or contractual / regulatory changes and performance indicators.

Third Party Risks

- Third parties acting on behalf of AGE UK STW, who are to have access to Data Assets; shall be required to be approved by the senior management.
- The approval process shall ensure Third Parties with access to 'Personal Data' for processing, that prior to processing a compliant Data Processing Agreement is in place.
- The requirements of this policy shall be levelled on all sub-contractors and suppliers with whom Personal Data relating to customers, staff or volunteers is shared; through the provisions of Data Processing Agreements.
- The Supplier approval process shall also consider the requirement to audit contractors who are not able to demonstrate approved / certified data security systems & controls.
- The sharing of personal data with any organisation located in a country outside of the EEA and which does not have an EU 'Adequacy Decision'; will be only be permitted when a Data Processing Agreement which includes 'Standard Contractual Clauses' has been put into place with them. These organisations must also be able to demonstrate adequacy in the protection

of individuals freedoms and rights. The DPO needs to be consulted prior to engagement with this type of organisation.

A1.4 Change Management

- Changes to Process Facilities, Equipment, IT Systems and Service provision shall only be conducted with prior approval of senior management following review of proposed changes and assessment of potential data security risks.
- The review process shall also consider potential for high-risk processing with impact on data subjects rights. The Project Initiation document shall be used for all changes, to ensure that the processing risks are considered and a Data Privacy Impact Assessment conducted as appropriate using the Change Management policy and control form in this document (Appendix 6).
- New systems or developments / amendments to existing systems shall be tested in isolation from the operational system (as applicable) to ensure they meet functional and security requirements, prior to release for operational use. Access to such systems or equipment shall only be permitted to authorised staff or contractors, in order to prevent unauthorised access and changes occurring.

A1.5 Business Continuity Planning (BCP)

- The senior management team shall determine suitable contingency to ensure continuity of data security and service provision, in response to the effects of unplanned events or failures.
- Contingency planning shall be incorporated into the risk assessment process and the risks of disruption or security compromise be factored into the requirement to treat identified unacceptable risk.
- The senior management team will be responsible for the periodic testing of planned contingency measures to ensure their adequacy and effectiveness in providing continuity of Data Security and service provision.
- Business continuity planning shall also ensure that AGE UK STW has adequate insurance cover for losses, legal costs and damages which may be incurred as a result of a data breach and/or Cyber-attack.

A1.6 Data Classification, Handling & Retention

- All Personal Data & Business Data shall be classified ‘Confidential’ and shall be handled in accordance with the requirements of this policy document.
- It is the responsibility of all staff or volunteers to apply the requirements of this policy document to any data they are given access to and are responsible for.
- All data in use shall be held in files specific to the client or business activity and ensures their segregation.

- All other electronic data not held for retention purposes within the allocated share file, shall be deleted from files / devices on completion of its use.

- Electronic data transferred via E mail should not be held in storage within E mail accounts and should be deleted following extraction or copying of the required data. (This includes Trash / Delete folders)

- All Data shall be retained in accordance with the defined periods specified in the Retention & Disposal Policy (Appendix 4). Which shall ensure data is not retained beyond required contractual or legal requirements.

- Personal Data retained shall be minimised to only that as required to meet contractual or legal requirements.

- Electronic data storage media on disposal shall be subject to data erasure using nationally (NCSC) approved software or physical shredding to 30mm particles or less.

- Electronic data disposal services shall only be procured from contractors holding valid certification to ISO27001 or ADISA standards and as approved by the senior management.
- Hard copy data shall be shredded utilising a shredder meeting DIN level 4 as a minimum. All hard copy shredding shall be conducted through AGE UK STW facilities or by individuals at home via a specific Home Working Agreement.

- The requirements of this policy shall also be levelled on all sub-contractors and suppliers with whom Personal Data relating to customers is shared; through the provisions of Data Processing Agreements.

A1.7 Personnel & Access to Data Assets

- All staff and volunteers shall be subject to Confidentiality Agreements.

- All staff and volunteers shall be issued the Data Protection / Security & Acceptable Use Policies and agree to their requirements

- Relevant personnel screening / DBS checks and reference checks will be conducted on staff or volunteers prior to access to customers or their personal data.

- Access to identified data assets shall only be granted with the prior approval of senior management. Access shall be granted on the basis of it being needed to perform job role, which may be for a restricted time if not permanently required.

- Physical access to data assets by staff and volunteers shall be restricted as practical.

- Staff and volunteers shall not allow access to any other individual (including family members) whilst working remotely.

- It is a **mandatory** requirement on all staff and volunteers, that they inform senior management of any changes in their personal circumstances or if they commit an offence. All changes are to be reported by staff regardless of whether they believe it is relevant or not, to their suitability for access to data assets.

- It is a **mandatory** requirement of all staff and volunteers to declare any known or potential 'Conflict of Interest', which relates to their own or direct family members circumstances, which would have bearing on their suitability to be granted access to AGE UK STW customer, staff or commercial data.

- Access to data held electronically on company IT systems, shall be via the use of unique user login credentials; in order that if required user activity can be reviewed. AGE UK STW reserves the right to monitor all user activity on its IT systems.

- Physical access to data assets by staff shall be restricted as practical. All visitors to site(s) shall always be accompanied, whilst onsite. All exterior access points shall be closed when not guarded / attended by staff.

- Staff and volunteers shall be responsible for ensuring that whilst working in any environment where non unauthorized persons are present (E.g. Public places / meetings / home), that Confidential data cannot be viewed or accessed by them.

- Access to all AGE UK STW data shall only be through company provided / owned equipment or software. The use of personal equipment or software is not permitted.

A1.8 Training & Awareness

- Senior management shall ensure that all staff and volunteers receive adequate levels of awareness training in data security policies, controls and relevant threats.

- All staff and volunteers shall receive as a minimum basic awareness training at employment induction and all staff receive refresher training annually.

A1.9 Internal Audit & Performance Review

- The senior management will undertake periodic Internal Audits and/or reviews of implemented data security controls; in order to verify compliance of staff and/or volunteers with Data Security Policies.
- The senior management team is responsible for the periodic review of performance in maintaining Data Security requirements, legal and contractual compliance.

A1.10 BYOD / Remote Working Policy

Staff must adhere to our Acceptable use of remote devices policy (A2.7 below) as well as ensure that all data storage and access principles are followed below in A1.10.

A1.11 Data Storage and Access

Electronic Data

- All Personal data and commercial data will be stored in secure servers which are encrypted. (Network & Charity Log)
- Connection to servers and data transfer shall be encrypted. (TLS)
- All access devices (PCs / Laptops) shall be encrypted.
- Access to Network files & Charity Log will only be through SMT approval.
- Access to Network / Charity Log shall be restricted to only those files needed by users.
- User device access shall be through unique identification and password.
- User passwords are required to be complex, a minimum 12 Characters and a combination of Letters, Numbers, Symbols
- Access to Network / Charity log shall be through unique identification and password.
- Administration access to the servers shall be limited to nominated administrators & requires unique authentication. (Two Factor Authentication where possible)
- All mobile phones used for business purposes shall require the individuals unique pin or fingerprint and will only be able to access information approved by the organisation, such as Wildix

- Users shall not keep a record of their login credentials (Paper/ Electronic) anywhere.

- Administrator accounts shall only be used for Administrative purposes only, these accounts shall not be used for access to the internet or email.

- Senior management shall periodically review administrator and user access permissions.

- All data which is required to be maintained and backed up, shall be held on the Network / Charity Log. User devices will not be backed up.

- No user devices shall be left in vehicles unattended / overnight.

- E mail accounts & user devices shall not be utilised for storage of data.

- Personal mobile phones shall only be utilised for e-mail or network access with the approval of Senior management and on a restricted basis.

- Personal mobile phones shall not be utilised for the storage of any AGE UK STW data.

Hard Copy

- Hardcopies of Personal data shall be kept to minimal required and destroyed a soon as possible afterwards.

- Hardcopy data secured when not in use – locked cabinets / drawers / case. (Including remote / Home Working)

- No documents shall be left in vehicles unattended / overnight.

- Hardcopies shredded following use – office shredder only, unless specified otherwise via a Home Working Agreement

- Hardcopies issued only on SMT approval on a need-to-know basis.

Data Transfers

- Transfer between the Network / Charity Log & devices shall be encrypted.
- Data transfers via E mail using TLS & documents password protected.
- Hard copy documents containing personal data shall only be despatched by post, where this is essential e.g. posting benefit forms..
- All transfers to Third Parties made under conditions of a Data Processing Agreement

A1.12 Internet / Cyber Security

- Servers shall be protected by a corporate level firewall, AV / Malware & monitored.
- All PCs / Laptops shall be protected with Anti-virus & Malware software.
- All PCs / Laptops shall have a Firewall installed.
- All PC / Laptop AV & Firewall updates shall be installed automatically on connection.
- All PCs / Laptops shall be installed with WIN 11 & automatically have security updated on connection.
- All staff and volunteers are subject to Acceptable Use Policy (Appendix 2)
- Wi-Fi networks shall be segregated & firewall protected.
- All user access to the internet, shall only be via the Network.
- Websites & files shall be scanned on access by AV/Malware.
- All Home routers in use shall have their default passwords changed by the user. Passwords reset by user shall be complex. (see above)
- Remote connection to the network shall only be made via the installed login portal provided on user devices.

- Remote access to the internet shall only be permitted via trusted and secure connections / Wi -Fi. Publicly available connections or Wi-Fi networks shall not be used to connect to the internet for work purposes.

A1.13 Data Back Up & Continuity

- All server data shall be backed up daily to alternate storage and held securely.
- All data back-ups shall be monitored for completion.
- Back Up copies shall be tested by the SMT for restore periodically.
- SMT shall ensure adequate Cyber/ Data Insurance cover will be maintained

A1.14 Physical Security

- All data processing shall be conducted in secure locations with restricted access.
- All devices & hardcopy data shall be held in secure buildings.
- Devices and documents shall not be left unattended or accessible. (Clear desk)
- Devices shall be turned off or locked when not attended.
- Screen saver / sleep mode shall be set at a maximum 5 minutes.
- A register of all IT assets in use shall be maintained.

APPENDIX 2 – ACCEPTABLE USE POLICY

A2.1 Introduction & Scope

The use of the email system, the internet and all forms of electronic communications within this organisation are encouraged, as this use facilitates communication and improves efficiency. Inappropriate use, however, causes problems ranging from lack of productivity to potential legal claims against the organisation.

The majority of our employees have access to electronic media and services, including computers, email, online services, the internet, online telephony and the organisation's intranet. This appendix to the policy sets out the organisation's guidelines on the correct use of email, internet, electronic communications and the organisation's response to inappropriate use under the following categories:

- Email
- Internet
- AI Software
- Social Media
- Remote Devices
- Telephone services

Electronic media, phones and services are provided by the organisation primarily for employees' business use. Limited, occasional, or incidental use (sending or receiving), for personal non-business purposes is understandable and acceptable. All such use should be done in a manner that does not negatively affect the use of the organisation's systems for business purposes. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

The organisation reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other policies of the organisation. Employees should not assume electronic communications are totally private. Accordingly, if they have particularly sensitive information about individuals to transmit, they should ensure this is secure by the use of the appropriate passwords or encryption.

A2.2 Acceptable Use of Emails

The email system is available for communicating matters directly concerned with the business of this organisation.

The style and content of email messages must be consistent with the standards that this organisation expects from written communications.

To reduce email overload and aid productivity, email messages should only be sent to those employees for whom they are relevant. Send blind copies (Bcc) wherever

possible and do not automatically reply to all names on a 'Cc' list. Only send attached files where absolutely necessary.

Under data protection law, email addresses can be considered as personally identifiable information, therefore if sending group emails, you should always Bcc all recipients.

Although email encourages rapid communication, the contents of email messages should be written with care as messages sent without proper consideration can cause unnecessary misunderstandings. Email should not be used as a substitute for face-to-face communication. Please consider the volume of email received by colleagues and only send when essential and do not copy all unless necessary.

Consider the data protection implications, do not use subjective comments or opinions in emails.

Where necessary, email messages should include a confidentiality statement.

All messages sent outside this organisation should include the standard disclaimer on your footers and should be updated as and when required.

Offers or contracts transmitted via email are as legally binding on the organisation as those sent on paper.

Email contact lists are the property of the organisation even if created by the employee. Employees may not copy or remove any contact list in its entirety for use outside the organisation without the express permission of his or her line manager.

In line with Principle 5 of the Data Protection Act information should not be stored for any longer than is necessary so it is important the employee regularly tidies up their emails and deletes any files no longer required. It is a requirement that all staff comply with the annual clean-up of their data including emails.

In the event of a Data Subject Access request any emails kept on the data subject will have to be disclosed. It is an offence to delete these after a subject access request has been made.

Any failure to follow these guidelines satisfactorily can result in disciplinary action up to and including summary dismissal.

A2.3 Acceptable use of the Internet

Unless it comes from an official source, information obtained from the internet (generally the World Wide Web) should be cross-checked before being used. Where that is not possible, full details of the source should be recorded.

Even when used for work-related purposes, browsing the web can be highly time-consuming and therefore should always be undertaken responsibly.

Any unauthorised use of email or the internet may result in disciplinary action, which may include summary dismissal.

Unauthorised Use

The organisation will not tolerate the use of the email or internet system for illegal or inappropriate activities. Such activities include (but are not limited to):

- Sending or forwarding any message that could constitute bullying or harassment (e.g. on the grounds of sex, race or nationality, religion, sexual orientation, age or disability).
- Non-business use, including personal messages, jokes, cartoons or chain letters.
- Posting confidential information about other employees, the organisation or its customers or suppliers (this includes any negative or derogatory statements posted from the employee's home computer and/or in the employee's own time).

Whilst PC equipment is provided primarily for communications relating to the official work of Age UK Shropshire Telford & Wrekin (Age UK STW), it is acceptable for employees to make reasonable use of computer facilities for non-official purposes, subject to the rules and safeguards set out in this code.

The term 'reasonable' cannot be fully defined and as such is open to a degree of interpretation. It is in this interpretation that users must exercise good judgement, as an abuse of such facilities could lead to a disciplinary action against the individual, and may result in the privilege being withdrawn for all. Examples of reasonable use may be: -

- Essential or occasional use only; preferably during non-work time.
- Occasional non-official internal email to friends or colleagues.
- Occasional non-official external email via internet.
- Occasional receipt of non-official email via internet.
- Occasional use of internet search facilities for reasonable personal interest or work related study material.
- Use of word processing to produce an occasional letter.

This organisation will not tolerate the use of the internet for illegal or inappropriate activities. Such activities include (but are not limited to):

- Online gambling.
- Accessing offensive, obscene or indecent material, including pornography.
- Downloading or distributing copyrighted information.
- Sending or posting abusive, rude or defamatory messages or statements about people or organisations.
- Online personal shopping or excessive use of the internet.

Monitoring

Monitoring and recording of email messages and internet use may be carried out as deemed necessary. Copies of email messages will be retained as appropriate.

Hard copies of email messages and details of internet sites accessed may be used as evidence in disciplinary proceedings.

Security

All users will be issued with (or will be asked to select) a unique individual password which will be changed at regular intervals and is confidential to the user. Access to the system using another employee's password without prior authorisation may result in disciplinary action, including summary dismissal.

Users must take all necessary precautions against the introduction of viruses into the system and not use any sites which may be considered unsafe. Users must ensure that critical information is not stored solely within the email system. Do not store information on your H drive. Information should be stored separately on the system personally identifiable information should always be stored in the appropriate files on the P Drive. If necessary, documents must be password protected.

A2.4 Acceptable Use of AI Software

Risks of using AI Software

We recognise the potential of Artificial Intelligence (AI) tools such as ChatGPT, Microsoft Copilot, and other AI-driven solutions to enhance productivity, efficiency, and decision-making. AI tools are to be used responsibly, aligning with our company values, legal requirements, and best practices in privacy, confidentiality, and data security.

There are several risks that must be considered when it comes to the use of AI:

Personal Data Protection: If users input personal information, it may unintentionally appear in generated outputs, risking privacy violations. All new AI tools must undergo a Data Protection Impact Assessment (DPIA).

Errors and Misleading Information: AI can generate incorrect or misleading content due to limitations in data quality, biases in training data or misunderstandings of prompts.

Unethical, Biased or nonsensical content: AI models can perpetuate stereotypes or political biases present in data, additionally they may generate content that is irrelevant, incoherent or offensive.

Inaccurate Legal Advice: AI can provide incorrect legal advice, often based on data from different jurisdictions or outdated laws and must not be used by the organisation for legal advice provision

Harmful Content Generation: Generative AI can produce and spread misinformation, manipulated media, or content that is insensitive to cultural differences or social norms.

Intellectual Property Risks: AI generated content can inadvertently incorporate copyrighted or trademarked material without proper attribution. Using copyrighted or protected material in training or output can breach IP laws. Organisations must

understand the data sources behind AI models and how that data influences content.

Cybersecurity: Generative AI can be exploited to conduct sophisticated cyberattacks. These models may also be manipulated to produce harmful outputs. Organisations must protect sensitive data, such as passwords, from being input into AI systems.

Use of AI

Prior to accessing or using AI tools, you must be assigned permission/a licence to use the AI tool by the IT department, following Senior Management Team approval. Employees and volunteers are not permitted to use AI tools without an assigned licence/permission, or through their own personal account for the AI tool. AI tools must only be used on secure, company-approved devices and networks.

Thorough Review: All AI generated content created by AI tools within the organisation must be carefully reviewed by a qualified staff member and ensure all content aligns with Age UK STW's mission and values. Generated content should be reviewed to ensure that the content complies with: -

- UK GDPR and Data Protection Act 2018 - Ensure no personal data is input. A DPIA must be completed for high-risk use cases.
- Intellectual property and copyright laws.
- Ethical AI usage principles, ensuring fairness, accountability, and transparency.
- Equality Act 2010 - Audit AI outputs for discriminatory bias especially in recruitment, marketing, or decision-making.

AI tools may be used in the following ways:

- Drafting non-confidential emails, reports, and summaries.
- Creating internal training (subject to review)
- Enhancing research and idea generation sessions.
- Supporting coding, debugging, and software development.
- Automating repetitive tasks to improve efficiency.
- Assisting with content refinement.

AI tools <u>must not</u> be used for:

- Processing, storing, or sharing business confidential information and IP, or Any form of personal data.
- Provision of legal advice for clients
- Avoid uploading proprietary company documents unless explicitly approved by the Data Protection Lead.
- Making final business decisions without human oversight.
- Generating misleading, biased, or harmful content.
- Engaging in unethical or unlawful activities.

General Guidelines:

- AI is to be used as an assistant, not a decision-maker.
- Always validate by subject matter experts and ethically review AI output before use.
- Clearly label AI-generated content.
- Keep records of prompts and outputs where material is used in a business-critical context.
- Use company-approved platforms with audit controls.
- Do not use AI to impersonate employees or external parties.
- Avoid overreliance and do not depend too heavily on AI at the expense of human judgement.
- Never use AI to replace regulatory consultation

Intentional and unintentional misuse of AI

Intentionally misusing generative AI systems is strictly prohibited. This includes any deliberate actions that breach ethical, legal or moral standards, potentially endangering the safety, privacy or security of older people, our staff, volunteers or the wider community.

Staff may use AI tools in ways that unintentionally cause harm such as producing inaccurate information, inappropriate content, bias or content that breaches data protection or copyright law.

Reporting Misuse

All Age UK STW staff are encouraged to report any suspected misuse of generative AI whether intentional or unintentional, to their line manager or another appropriate person. Reports can be made anonymously and will be treated confidentially. Any breach of this policy may lead to disciplinary action up to and including dismissal.

A2.5 Cyberbullying

This organisation has a zero tolerance policy towards all forms of bullying and harassment and this includes bullying using technology such as mobile phones, social media and computers whether it takes place within the workplace, or outside. As with other forms of bullying, cyberbullying is prone to being driven by prejudice. The organisation is alert to the possibilities of sexist, racist and homophobic cyberbullying. Any employee found to be in breach of our policy will be subject to the disciplinary procedure and disciplinary action could include dismissal.

Cyberbullying may include (the list is not exhaustive):

- Sending offensive emails to a colleague, even if this is meant as a joke, and continuing to send similar messages, having already been told to stop.
- Email threats, this might also include ostensibly inoffensive messages in terms of actual content where it is the implied meaning behind the message

that constitutes a form of bullying. An example of this might be where a manager is using email to bombard an employee with more work than they can handle, while other members of the team are not being treated in the same way

- Posting work related blogs and leaving comments on social networking sites. It may be that a person does not experience any direct form of cyberbullying being unaware that the bully is posting offensive messages about him/her on sites in the public domain.
- Propagating defamatory gossip about employees or volunteers on social networking sites and blogs.
- Threats or offensive comments sent to a person's mobile phone
- Harassment by email, sending persistent emails to a person when previous email approaches have been rejected.
- Sharing a person's private data online, posting someone's personal details, i.e. those which they would not normally want to share with complete strangers, such as home addresses and phone numbers, in such a way that they become available to the general public.
- Picture/video clip bullying via mobile phone cameras.
- Chat room bullying.
- Bullying via websites.

A2.6 Acceptable Use of Social Media

The organisation recognizes and accepts that its employees may keep personal blogs on their own internet sites and that internet social networking sites such as Facebook, What's App and X are a useful way of interacting socially with colleagues and friends. In addition, the use of social media sites are a good way to promote the charity's work and fundraising and as such staff are encouraged to do so.

Whilst the organisation does not wish to prevent employees from accessing such sites during lunch breaks whilst at work, nonetheless it expects certain standards of conduct to be observed, to protect both its legitimate business interests and its employees from the dangers of inappropriate use. This policy applies both inside and, in certain circumstances, outside the workplace.

- Employees must not access social networking sites for personal use during working hours. Access using the organisation's IT systems is restricted to lunch breaks and before or after the working day, unless specific permission is granted by your line manager.

- Employees must make it clear when posting information or comments on social networking sites that any views which are expressed do not represent those of the organisation.

- Employees must not divulge or post information on a social networking or social media site which is confidential to the organisation, its suppliers or customers.

- Employees must not make inappropriate reference to the organisation on a social networking or social media site to its employees, its customers, its suppliers.

- Employees must not post entries on a social networking site which are derogatory, defamatory, discriminatory or offensive in any way, or which could bring the organisation into disrepute.

- Employees should be aware that social media services or blogs may create documents which the courts can order to be disclosed for use in litigation.

- The organisation will monitor its IT systems as is deemed necessary in order to prevent inappropriate usage. Hard copies of blog entries may be used in any disciplinary proceedings.

- The above principles apply equally to information or comments posted by employees from their home, or other personal computers, and irrespective of whether the posts are done during working hours or in the employee's own personal time.

- Employees whose conduct breaches this policy in any way may be subject to disciplinary action in accordance with the organisation's disciplinary procedure, up to and including dismissal.

- The organisation recognises that it is possible to use social media and the internet to access information about potential employees, volunteers or clients. Employees must not use social media, or the internet, to check or find out information about potential staff, volunteers or clients. In the event that an employee has a concern about an individual they must discuss this with their line manager and must not use electronic media to access information about individuals.

Recommendation:

- It is best practice not to have your employer visible to the public in your profile; if its publicly visible then anything you post on the platform can be associated with Age UKSTW and runs the risk of either a) bringing the organisation into disrepute (see bullet point 1 above) or b) offending someone with views that differ from your own, which may result in a complaint or concern being raised by the viewer.

- It is recommended that you review your public-facing profiles on social media platforms such as Facebook and X and adjust your privacy settings either to remove your current employer completely or restrict it to 'friends' only. Failure to do so risks the outcomes set out above.

A2.7 Acceptable Use of Remote Devices

Remote devices may include smartphones, laptops, tablets and any other electronic devices

Employees may be provided with a mobile telephone, a laptop or a tablet where it is deemed necessary in the course of their work or for homeworking. Staff should remember that this equipment remains the property of the charity and can be recalled at any time if required.

Work mobile phones should be used purely for work-based calls. However, it is recognised that it may be useful for staff to use their own laptops or tablets for other activities, not directly work related. This is acceptable provided those activities are not illegal in any way, compromise the security and reputation of the organisation or likely to cause any damage to the equipment.

The purpose of this appendix to the policy is to establish an authorised method for controlling mobile computing and storage devices that contain or access information resources at Age UK STW. With advances in computer technology, mobile computing and storage devices have become useful tools to meet the business needs of the organisation and enhance staffs working environment. However, these devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere. As mobile computing becomes more widely used, it is necessary to address security to protect information resources.

It is the policy of Age UK STW that mobile computing and storage devices (e.g. laptops, tablets, smartphones) containing or accessing information must be approved prior to connecting to the network and this includes equipment used for home working. This requires the approval of the person's line manager and a formal Home Working agreement. A record of all equipment used for home working is kept by the Director of Finance, and loss failure of theft of this equipment must be reported immediately. Access to work mobile devices must not be given to individuals outside of the organisations, such as family members.

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network. They must be fully password protected at all times and it is imperative that staff using mobile computing devices ensure that they are safeguarded at all times.

- All devices which can access the P drive must have strong passwords with at least 12 characters letters, one symbol and a number. These must not be shared, except with your line manager in the event of ill health or an emergency and changed afterwards.
- Access to mobile devices including work mobiles should also be password protected in the same way as 6.1.
- If using Wildix on your own mobile device, or accessing outlook you must ensure your phone has strong security and that these cannot be accessed by anyone else.
- No client personal data should be stored on staff's own mobile phones. Staff with access to Microsoft outlook on their personal phones should regularly delete e-mails

- All laptops which contain personal data must be encrypted and the data must be removed the minute it is no longer needed. This is the responsibility of the staff member using this device.
- Any tablets or similar devices should not contain personal data, this should be accessed via the P drive with strong password protection as above.

It should be noted that it is not just personal data which can be sensitive, some information may be commercially sensitive to the organisation. As such all data that is stored on mobile computing devices, not just personal data, should be encrypted and password protected

Appendix 3 – Data Subject Access Request Procedure

A3.1 Introduction

Individuals (known as data subjects) have a right to obtain, from the data controller, confirmation as to whether their personally identifiable data is being processed and, where that is the case, request access to the personal data.

The means by which an individual can make a Data Subject Access Request is outlined within the AGE UK -STW Privacy Notices which can be found here:
P:\Organisation & Governance\Data Protection & GDPR\Privacy Notices
The request to exercise this right is typically called a "Data subject Access Request" or DSAR.

This policy is presented as the process by which AGE UK - STW will action such requests to ensure that the rights of the individuals are protected.

In order to provide a timely response Age UK STW has access to the support of their external Data Protection Officer (DPO) Amicis Data. Liaison with the DPO will be via their helpdesk support team using the assigned email:
AgeUKShropshireandTelfordDPO@AmicisData.com

This policy applies to all trustees, directors, employees or volunteers that may collect, process, or have access to data (including personal data and/or sensitive personal data). It is the responsibility of all the above to familiarise themselves with this policy and ensure adequate compliance with it.

Definitions

Data Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Data Subject	The identified or identifiable living individual to whom personal data relates.

Data Subject Rights

RIGHT	EXPLANATION
RIGHT TO BE INFORMED	This means that we must be transparent in how we collect and use personal data
RIGHT OF ACCESS	Individuals have the right to access their personal data.
RIGHT TO RECTIFICATION	If the information we hold about them is inaccurate or incomplete, they can request that we correct this
RIGHT TO ERASURE	Individuals can request that we delete or remove personal data in certain circumstances
RIGHT TO RESTRICT PROCESSING	Individuals have the right to request that we cease processing their data if: • They consider it inaccurate or incomplete and/or • They object to the reason we're processing their data We will review the validity of their request and respond with our decision
RIGHT TO DATA PORTABILITY	Where they have consented to our processing of their data, or where the processing is necessary for us to deliver a contract, they can request a copy of that data be provided to a third party
RIGHT TO OBJECT	Individuals have the right to object to our processing in certain circumstances.
RIGHTS RELATING TO AUTOMATED DECISION-MAKING INCLUDING PROFILING	We do not use automated decision-making or profiling. Where automated decision-making is applied, organisations must provide information about the processing; introduce simple ways to challenge the decision or request human intervention; and carry out regular checks to make sure that systems are working as intended.

A3.2 DSAR Process / Recognising a DSAR

There is no specific format required to initiate a request for a DSAR. Requests can be made in person, by telephone, by letter, email, online chat facility and even by social

media post. Where we are the data controller, we have a template form that can be easily completed by the data subject and collects all the information required for a swift response, this is stored here: -

P:\Organisation & Governance\Data Protection & GDPR\Subject Access requests\ICQ6 - DSAR REQUEST FORM.docx

This form is not compulsory and should only be used when the data subject has not provided enough information for you to carry out the request and complete the form yourself.

Certain requests fall within our normal business practices and should be actioned accordingly. For example, a simple request to be removed from a mailing list (unsubscribing) or updating personal details, can be actioned immediately and confirmation sent to the data subject. Once you have identified a data request, you must determine if we are the data controller or data processor and follow the instructions below.

A3.3 DSAR requests where AGE UK-STW are the Data Processor

Where we are processing data under the instructions of the data controller, we must pass on the request as soon as possible. Any data processing agreements in place oblige us to forward the exact request immediately and without undue delay.

In the event of such a request, please inform the CEO who will forward the request to the relevant party as per the terms set out in the data processing agreement. AGE UK -STW will cooperate with data controllers to enable them to comply with any exercise of rights by a data subject under data protection legislation.

A3.4 DSAR Process where AGE UK - STW are the Data Controller

In the event of a subject access request for data that we process as the data controller, the following process must be followed.

A DSAR will be processed without undue delay and within a calendar month of receipt and identity verification unless assessed as being particularly complex. In which case we will contact our DPO for guidance. A Service Level Agreement (SLA) within the DPO Support Desk currently exists to conclude DSARs within 20 working days. Fees may not be charged for providing information to individuals in response to a subject access request. If we receive a DSAR that is 'manifestly unfounded or excessive', we may charge a reasonable fee to deal with the request or refuse to provide information. We will consult our DPO for guidance.

A3.5 Dealing with requests

Upon receipt of a request for personal data, the CEO will be notified. If more information is required to complete the request, a DSAR request form may be sent to the data subject. Staff or Volunteers should not attempt to address the DSAR themselves. Please note that a verbal request is a valid form of DSAR and therefore a data subject cannot be forced to put it in writing.

If deemed complex or unusual, CEO may choose to contact the DPO for advice and guidance via the dedicated DPO email address:
AgeUKShropshireandTelfordDPO@AmicisData.com

A3.6 Identity Verification

Before accepting a request, it is necessary to verify the identity of the data subject. If there is any doubt, photographic ID may be requested.

Identity may be confirmed in the following ways:

- data subject known to personnel
- verbal verification, by asking the data subject to provide personal details that match those held on their record e.g., DOB, Address etc.
- where the request will be sent to (email or postal address) matches that recorded on the data subject's file; or
- by confirming that the details on photographic ID provided, matches those on the data subject's file.

Once identification is confirmed, we might refuse the request on specific grounds. If rejected, the CEO will inform the DPO of the grounds for rejection, and they will provide guidance on communicating this with the data subject. It is not expected that any reasonable request will be refused and so we commit to responding to all accepted requests **without undue delay and, at the latest, within one calendar month.**

A3.7 Processing the DSAR

Once we receive the request and identity has been verified, CEO or the DPO will assign a reference number and note it in the DSAR log. This reference number will be communicated to the data subject with any communications relating to the request.

The CEO will co-ordinate export of any electronic data from the data subject's record. Paper records will be scanned and provided for full DSAR electronic requests. For postal requests, a copy of the record will be sent, and original documents must be retained.

When sending data to the data subject, we will provide a covering letter to accompany the data transfer, this should include a link to the privacy notice on the website or, the CEO may choose to use the CDPO template: -

P:\Organisation & Governance\Data Protection & GDPR\Subject Access requests

AGE UK – STW is responsible for the execution of the request and will notify DPO to confirm completion. If any causes may preclude the deadline from being met, then we will inform the DPO Support Desk, who will provide guidance on informing the data subject about the delay.

Sending Data

Where sharing data forms part of the request, we will ensure the security of data in transfer between us and the data subject/3rd party. The transfer method employed shall be agreed with the Data Subject.

Electronic transfer

If providing the data electronically, we will use a secure transfer method which ensures that sensitive information is exchanged securely with Data subjects. This may include emailing password protected documents or providing secure access to a share file. The CEO will co-ordinate the secure transfer.

Collection:

The data subject will be informed when the data is ready to be collected. Their identity must be verified upon collection.

Post:

Postal responses will be sent by special delivery (tracked and signed for) at our expense. If acceptable to the Data Subject the data can be delivered in person by a member of staff.

A3.8 Logging DSARs

All requests are recorded in a DSAR log to keep track of the details of the request, the action taken, and the length of time taken to respond. We are responsible for the execution of the request and will present the DPO Support Desk with evidence to confirm that the request has been executed where their guidance has been followed.

A3.9 DSAR Retention

DSAR requests should be noted on the relevant data subject's file. Request forms should be securely destroyed after 12 months, and any photographic ID copies should be destroyed as soon as their identity has been verified and at the latest within 7 days of responding to the request.

Appendix 4 – Record Retention & Management Procedure

A4.1 Introduction & Purpose

This appendix is the Record Retention and Management procedure for Age UK Shropshire Telford & Wrekin. This process sets out the principles and procedures relating to the retention, archiving, retrieval, and destruction of both electronic and paper records within Age UK STW. Each Service area must implement and adhere to this process.

This procedure is not only about record retention. Retaining records is of little use unless they can be retrieved, when necessary, in a timely and efficient manner, in accordance with Age UK STW business, legal and regulatory requirements. Certain retained records must be destroyed, after an appropriate retention period, to ensure that only appropriate records are retained and to manage retained records efficiently to minimise storage costs.

A4.2 The Process and Record Retention Schedule

To facilitate compliance with this Process, a Record Retention Schedule is stored here: -

P:\Organisation & Governance\Policies & Procedures\AUSTW.Policies\Information, data protection and GDPR polices and procedures\Records Retention Schedule V8 Dec 25.docx

A4.3 What is a record and why do we keep them?

A record is any information created, received, or maintained as information or evidence by Age UK STW in the course of its business, or to meet legal or regulatory requirements. This applies to records in all formats; compliance is required with the Companies Act, Data Protection Act, Charities Act, HMRC and Service Level Agreements/Contracts that AGE UK STW may have. Sensitive data should only be collected on a need-to-know basis.

Why does Age UK STW need a record retention process and schedule?

Records need to be retained, archived, retrieved and destroyed to comply with the statutory and regulatory requirements of the following examples of legislation:-

- Data Protection Act 2018
- Companies Act
- Charities Act
- HMRC
- Fraud Prevention

Age UK STW may be required to produce records for the following purposes:

- complaints handling
- regulatory investigations
- litigation
- internal and/or external audit or compliance
- managing relationships with third parties
- for business requirements (for example, dealing with customers)
- data subject access requests; and
- to demonstrate its compliance with its corporate and regulatory obligations.

Consequently, it is essential for Age UK STW to have an effective and robust records management culture which:

- ensures that Age UK STW complies with its legal, regulatory, best practice and commercial obligations
- ensures that Age UK STW can meet its business requirements
- includes procedures for efficient storage and fast retrieval of records
- improves Age UK STW's operational efficiency; and
- keep storage costs to a minimum.

Age UK STW must ensure that its record retention is in line with the Data Protection Act principles and individual rights enshrined in the principles, in particular:

- the right to be informed – what information is retained and why
- the right of access – individuals have the right to access the information held about them
- the right to rectification – individuals have the right to rectify incorrect information
- the right to erasure - individuals have the right to have their information erased
- the right to restrict processing - if the individual no longer wants us to process their information
- the right to data portability - if the individual wants to take their data elsewhere
- the right to object - to the processing if their information
- the right not to be subject to automated decision making – not applicable to us

The six Data Protection Principles are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)

A4.4 Retention of records

What form could a record take?

A record can be in any format (such as paper, electronic, microfiche, images, video & audio recordings etc.) and, for example, can be evidence of:

- an action taken, for example a referral transaction.
- analysis of a service issue or of decision-making within the organisation, for example, board papers or board minutes or e-mail exchanges; or
- a record of a meeting, for example, minutes of a meeting.

What records must I keep?

A record must be kept if it could be used, for example:

- to evidence the decisions which are made in the business or its performance (project records such as business plans, budgets, financial preparations for the annual report and accounts and financial projections and management information); for the Companies Act, HMRC, Charities Act and Data Protection Act
- for regulatory investigations (e.g. HMRC or ICO), such records could include payroll records, VAT receipts and gift aid forms, client or staff records
- for legal claims and agreements (contracts, partnership agreements, external correspondence, project documentation);
- to comply with the Companies Act
- for employee issues (personnel records) and/or the Equality Act 2010
- for customer-related issues (complaints, customer contact); and /or subject access requests under the Data Protection Act
- for tax reasons (for example, for VAT, Gift Aid, PAYE tax audits and/or HMRC investigations).

If you are in any doubt as to whether any information or documents need to be retained as records, you should contact your line manager or the Chief Executive.

In all cases, records must be retained, archived, retrieved and destroyed in accordance with this Record Retention Schedule and process.

How long must I keep records?

All records must be kept for the length of time necessary to fulfil all Age UK STW's obligations, but no longer, and must be retained in line with Data Protection principles.

The records held by each service area must be kept in accordance with the retention periods contained here: -

P:\Organisation & Governance\Policies & Procedures\AUSTW.Policies\Information, data protection and GDPR polices and procedures\Records Retention Schedule V8 Dec 25.docx

The requirements of the Record Retention Schedule have been set to ensure compliance with Age UK STW's legal, regulatory and business requirements and, where necessary, agreed with Risk, Compliance, Finance and Corporate Governance.

The retention periods set out in the Record Retention Schedule take into account that a record may be required for a number of purposes and specifies the longest applicable and legally compliant retention period.

In the event that a retention period is not specified in the Record Retention Schedule, contact the Chief Executive, with the appropriate details, who will get the document added to the retention schedule.

Any exceptions to the requirements of the Record Retention Schedule must be approved by the Chief Executive in writing if relating to Data Protection legislation.

In what format should I keep records?

When thinking about how to keep a record, the format chosen should be the one which gives the most operational efficiency, allows easy retrieval, maintains the security and integrity of the record, complies with Age UK STW's obligations and is cost effective. The following should be considered:

- Some records must be kept in their original format. Where this is not necessary, it should be stored electronically.
- Where practicable, records should be retained in a format that prevents the record from being modified (password protected) or deleted (except under controlled circumstances).
- If a record is copied into another format such as scanning or electronic copy because it is not necessary to retain the original, the original record should be destroyed, provided that the imaged or electronic copy is kept for the full period specified in the Record Retention Schedule.
- When originals are not kept, record reproduction should be of a high quality. The quality of a copied record may impact our ability to use it in litigation or regulatory investigation.
- It is not necessary to keep duplicate copies. Only one easily retrievable, readable, high-quality record is necessary.

A4.5 Filing Records

Each service area must apply its filing procedures in a consistent manner. Such filing practices should cover how files are named and numbered, who keeps them, who can access them and where files are stored; this should be recorded in ISO Procedures

Files must be stored consistently and should be capable of being retrieved quickly and accurately.

Some records must be kept at the same location as their owner e.g., Board Minutes.

Records of the same type and with the same retention period should be filed together, where possible.

If your records are confidential, it is recommended that the principles below are followed:

- number pages sequentially, it will then be apparent if any have been removed or lost
- keep them securely with restricted access
- electronic records should be backed-up regularly; and
- dates should be clearly set for destruction of electronic records.

A4.6 Responsibility for records management

Every Age UK STW employee is responsible for ensuring that records are retained, archived, retrievable and destroyed in accordance with this procedure and the standards contained in the Record Retention Schedule.

A4.7 Transfer of records

There may be instances whereby original records are required to be transferred to another business unit or supplier or to a third party such as another service provider. Permanent or temporary transfers of records must be recorded formally by the DP lead with the support of the DPO. Evidence of the transfer together with any advice and correspondence must be saved here: -

P:\Organisation & Governance\Data Protection & GDPR\Data Record Transfers

A4.8 Destruction

All records must be retained in line with data protection legislation and must provide for the systematic disposal of electronic as well as paper records. There must be a legitimate reason for both the retention and destruction.

Review before destroying

If records, which are needed, have been destroyed, the courts/regulatory authority will look at the basis on which they were destroyed and whether this conforms to generally accepted practice. An adverse inference can be drawn from the absence of any record which could lead to serious consequences for Age UK STW and potentially the person responsible, so it is essential that all records are reviewed before they are destroyed.

Therefore, before records are destroyed you should consider whether the destruction should go ahead, in doing so you should take into account factors such as:

- whether there is any pending, threatened or ongoing dispute or claim not yet resulting in threat of litigation or regulatory investigation for which the record may be required
- whether the record is still being used or may be useful in the future
- whether there are historical or compliance reasons to keep the record
- if it is a contract, is it still in force or are there any ongoing obligations
- are there any Data Protection regulatory reasons for retaining, or destroying, the record

If you are in any doubt, you should consult your line manager or the Director of Finance before the records in question are destroyed. It may be a disciplinary matter to destroy records without properly referencing this process.

When destruction must not happen

Records known or suspected to be involved in a pending legal case or any regulatory investigation must not be destroyed.

Systematic destruction

It is essential that records are destroyed according to a documented and systematic process. Therefore:

- Records of the same category, which share the same date for destruction, should be stored together, where possible.
- In the unlikely scenario that records are stored off-site, all boxes must be clearly labelled with destruction dates. If some records are destroyed, and others are not without a proper reason, Age UK STW may be open to the charge of having destroyed records on a selective basis to escape possible liability rather than following sound prudent business practices.
- Systematic destruction must also apply to electronic records and any files, such as HR files, must be archived securely for the required timeframe with dates for destruction clearly marked on them

Means of destruction

- Records should be destroyed in accordance with the means specified in the retention schedule kept here: . P:\Organisation & Governance\Policies & Procedures\AUSTW.Policies\Information, data protection and GDPR polices and procedures\Records Retention Schedule V8 Dec 25.docx
- For locally held records, any confidential waste should be placed in the shredding bins provided around the building. Staff are responsible for shredding this waste as soon as is required.
- Any non-confidential waste must be placed in the recycling bins.
- Records must not be kept for any length of time longer than outlined within the Record Retention Schedule, unless identified as relevant to any legal or regulatory proceedings prior to destruction.
- Electronic client files on our CRM are destroyed by the Informatics Coordinator
- Paper and electronic HR files, and any related emails are archived and destroyed by the relevant line manager.

A4.9 Confidentiality and destruction of confidential waste

Confidentiality levels

Records should be allocated a level of confidentiality based on the information and/or data contained in the document. The level of confidentiality will be a factor in determining the storage standard for the document and its means of destruction as shown in the table below. As most records are now digitized paper storage should be kept to a minimum with most data stored electronically as standard practice. Paper records will only be kept if essential to do so.

Paper documents and other physical media

Confidentiality Level	Activity		
	Local Storage & Archiving	**Destruction**	**Secruity & additional measures**
Unrestricted	Held in File	Destroyed via normal waste disposal	None

Office Use Only	Held in file, with access restricted to Age UK STW personnel	Destroyed via normal waste disposal	None
Restricted	Held in file, with access restricted to certain nominated staff	Destroyed via confidential waste disposal	List of staff with access kept up to date
Confidential (HR volunteer, staff and client files)	Held in file under lock and key	Files Shredded / Confidentially destroyed	Access restricted to a small number of key staff

Electronic Documents

Confidentiality Level	**Activity**		
	Storage	**Destruction**	**Secruity & additional measures**
Unrestricted	Documents kept in shared area of the cloud drive	Delete from shared area	None
Office Use Only	Documents kept in shared area of the cloud drive	Delete from shared area	Restricted to users with access to those shared areas
Restricted	Documents kept in a folder within a restricted area of the network and password protected or encrypted	Delete from restricted Area	Access given by authorised person – i.e., not just anyone can request access to the restricted folder.
Confidential (HR volunteer, staff and client files)	Documents kept in a folder within a restricted area of network and password protected or encrypted	Delete from restricted area	Access given by authorised person – i.e., not just anyone can request access to the restricted folder.

A4.10 Disposal of Confidential Waste

For confidential waste the below principles must be followed

- Bins are provided specifically for shredding.
- Recycling bins must not be used for confidential waste, as it will not be securely destroyed.
- Rubbish bins (e.g. at each desk) and bins that are situated in public areas must not be used for confidential waste.
- On-site Confidential paper shredding / disposal is conducted utilising a shredder meeting DIN Level 4 standard.
- Once a year confidential paper shedding that is no longer required due to our retention schedule is disposed of through a qualified contractor
- Paper files are stored in the archive room with staff access only using a key code. This room must be kept tidy at all times.
- Electronic data and IT hardware devices such as, laptops and mobile phones must be encrypted, periodically assessed and data deleted as appropriate. All electronic data, including email, must be 'spring cleaned' on an annual basis, at a time specified by SMT.
- All data bearing IT equipment must be securely disposed of by a qualified contractor, holding certification to ISO27001 or ADISA standards and full traceability of all equipment provided.
- All Confidential waste disposal must be certified by contractors and records maintained.

A4.11 Disposal timetable

Confidential paper records. In June each year the organisation will have an annual clear out of all paper records identified for confidential shredding, unless the timescale for requirement of shredding is sooner.

Any non-confidential paper records which have not already been destroyed will be destroyed in June in line with the instructions above.

Electronic records. All electronic records will be reviewed in July each year, any no longer required will be deleted.

A4.12 Monitoring & Review

All staff are responsible for compliance with this process; such compliance will be subject to periodic review by the Chief Executive and reported to the Finance & Audit Committee.

The records retention schedule will be thoroughly reviewed annually or as needed by the CEO or a nominated SMT lead. Our retention schedule is saved P:\Organisation & Governance\Policies & Procedures\AUSTW.Policies\Information,

data protection and GDPR polices and procedures\Records Retention Schedule V8 Dec 25.docx

Appendix 5 – Data Breach Procedure

A5.1 Introduction

This procedure is provided for use by senior AGE UK – STW managers to assist in identifying Data Breaches and requirements for subsequent reporting to the DPO. The IG Lead or senior manager appointed by them, will be responsible for liaising with the DPO to investigate any actual or suspected Data Breaches which have been reported by staff, volunteers or third parties.

This procedure details the steps which need to be taken, to ensure that a Data Breach is handled in a controlled and contained manner, so that an accurate assessment can be made of its impact, applicable reporting and notification requirements correctly identified and any potential reputational damage limited.

A5.2 What is a Personal Data Breach?

All staff involved in a Data Breach incident must be aware of the need to contain communication of such events, both internally and externally as far as possible. The damage to an organisation through misleading information, over reaction or scare mongering; should not be underestimated and it is essential that senior managers control the situation until it has been thoroughly investigated and the facts established. It is important that staff responsible for the investigation or reporting of a Data Breach (actual or suspected), understand what may constitute a Data Breach in respect to Data Protection legislation.

A Personal Data breach is defined as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

In terms of breaches the Data Protection Act 2018 is applicable only where there is a breach of personal data and the respective potential consequences of it.

A5.3 Types of personal data breaches

Data Breaches with impact on Personal Data can be categorised as those having an impact on:

- Confidentiality – *"where there is an unauthorised or accidental disclosure of, or access to, personal data."*
- Integrity – *"where there is an unauthorised or accidental alteration of personal data."*
- Availability – *"where there is an accidental or unauthorised loss of access to, or destruction of, personal data."*

These core categories should be understood by staff , alongside the fact that a breach can affect one or more of these principles at any one time. Confidentiality is regarded as the easiest to detect and determine a breach of, whilst integrity is also relatively

clear in that regard. Availability has two aspects. The permanent loss, or destruction of personal data is an obvious breach, however availability issues can also be temporary. Legislation states that appropriate technical and organisations measures should have:

"the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;"

And:

"the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;"

Although the ability to restore access to or availability of personal data in a timely manner is an appropriate measure, the temporary loss of availability should be treated as a breach. Where careful consideration should be applied in assessing the potential impact to the rights and freedoms of natural persons. This is where the context of the data, processing activities and consequence of the breach should all be considered in determining potential impact.

A5.4 Potential consequences

There can be many adverse effects of a Data Breach, however, Data Protection legislation is focussed on the potential impact to the rights and freedoms of individuals (Data Subjects) as defined:

"may[....]result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

There is a lot to consider when determining the potential consequences of, or the risk that a personal data breach has to the rights and freedoms of individuals. It is therefore important that conclusions are not made without all the facts being known and the DPO has made an assessment of these.

The requirement to notify the competent supervisory authority (ICO) is only triggered where there is a risk of the above outlined adverse effects taking place.

In terms of communicating to the individuals, this is triggered where the risk of those adverse effects taking place is determined to be high.

The DPO will in liaison with the IG Lead, determine from the investigations which have taken place, whether the thresholds have been met for notification to the supervisory body and individuals. The DPO will then support AGE-UK STW in making any required notifications in the appropriate manner.

A5.5 Reporting Requirements

Internal Reporting & Investigation

The AGE UK-STW Data Protection Policy requires that all staff or volunteers who are aware of or suspect a data breach, shall immediately inform their line manager and/or the IG Lead.

Line managers should ensure that the IG Lead has been informed and that staff or volunteers reporting the incident are reminded of their responsibilities to treat this information as strictly confidential and not communicate it to anyone else.

The IG Lead shall make an initial notification to the DPO via the DPO helpdesk e mail, ensuring that they are aware of the situation and initial facts of the incident.

The IG Lead should then liaise with those managers and staff deemed necessary to form an investigative team, who will be responsible for ensuring that the required facts of the incident are gathered.

The Investigation team shall utilise the DPO Notification form: -

P:\Organisation & Governance\Data Protection & GDPR\Breaches\DPO Data Security Breach Reporting Form v1.2.docx

This will form the basis for the information required to be collected and subsequent actions needed to be taken. The DPO should be consulted at any stage, should support be required in completing the Notification Form.

On completion of the Notification form, the IG Lead will submit this to the DPO for assessment and determination of further reporting requirements and mitigation of risks.

It is vital that from the point of the initial awareness that a Data Breach has or may have occurred that the investigations are completed swiftly. Should the Data Breach be reportable under legal requirements there is only a short time allowance of 72hrs. (See below)

A5.6 External Reporting to Supervisory Authority

Should a Data Breach be assessed by the DPO and IG Lead to be reportable under legal requirements, then this reporting will be made by them to the ICO. It is important to note, that should the Data Breach have occurred at another organisation, who is a Data Processor to AGE UK -STW, it remains the responsibility of AGE UK-STW as the Data Controller to determine if the Breach is reportable and make such reports to the ICO.

The legal requirements state:

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is

unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

There is a certain amount of ambiguity as to when a Data Controller becomes aware a reportable Breach has occurred, as clearly some investigation is required to confirm this. Further guidance has suggests:

"has a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised."

In situations where there is some uncertainty as to whether there will be impact on individuals rights and freedoms and more time is required to establish this; the DPO will make an initial report to the ICO and a phased approach to reporting adopted.

The DPO in liaison with the IG Lead, will ensure that the information required by the ICO under legal requirements is fully met.

A5.7 External Reporting to Individuals (Data Subjects)

The DPO and IG Lead will determine the requirement to notify individuals of a Data Breach which has impact on them and the time scale of this.

Where a consequence of a personal data breach results in a high risk to the rights and freedoms of individuals the law dictates an obligation to inform the data subjects:

"Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the date subject without undue delay"

This notification is in addition to the obligation to inform the supervisory authority. There is no direct timeframe for such notifications other than the term 'undue delay'.

The notification should provide specific information in order that the data subjects are made fully aware of the breach and the steps that they should take to protect themselves.

Due to the nature of the breach and the risk to individuals it may be the case that notification to the individuals needs to be done before notifying the supervisory authority, where action is time critical in the protection of those individuals.

The notification to the data subject should be communicated directly with them, unless the effort to do so would be disproportionate. In which case a public communication, or similar measure may be employed.

Notifications to affected data subjects should be undertaken in close cooperation with the supervisory authority, respecting any guidance provided by it, or other relevant bodies, for example law enforcement.

A5.8 Data Breach Response

In addition to determining how and when the Data Breach occurred, it will be important that those Senior management and staff nominated to the investigatory team; also consider immediately what measures are required to prevent any further compromise of data security or availability.

Measures need to be identified and implemented to ensure that all steps necessary are taken to mitigate the impact of the breach as quickly as practical. This may require the temporary suspension or closing down of certain activities or data processing systems, but it is important that the need to protect personal data and data subjects, overrides commercial priorities.

It will be equally important to understand exactly how the incident occurred, in order that preventative measures can be introduced to stop any re-occurrence.

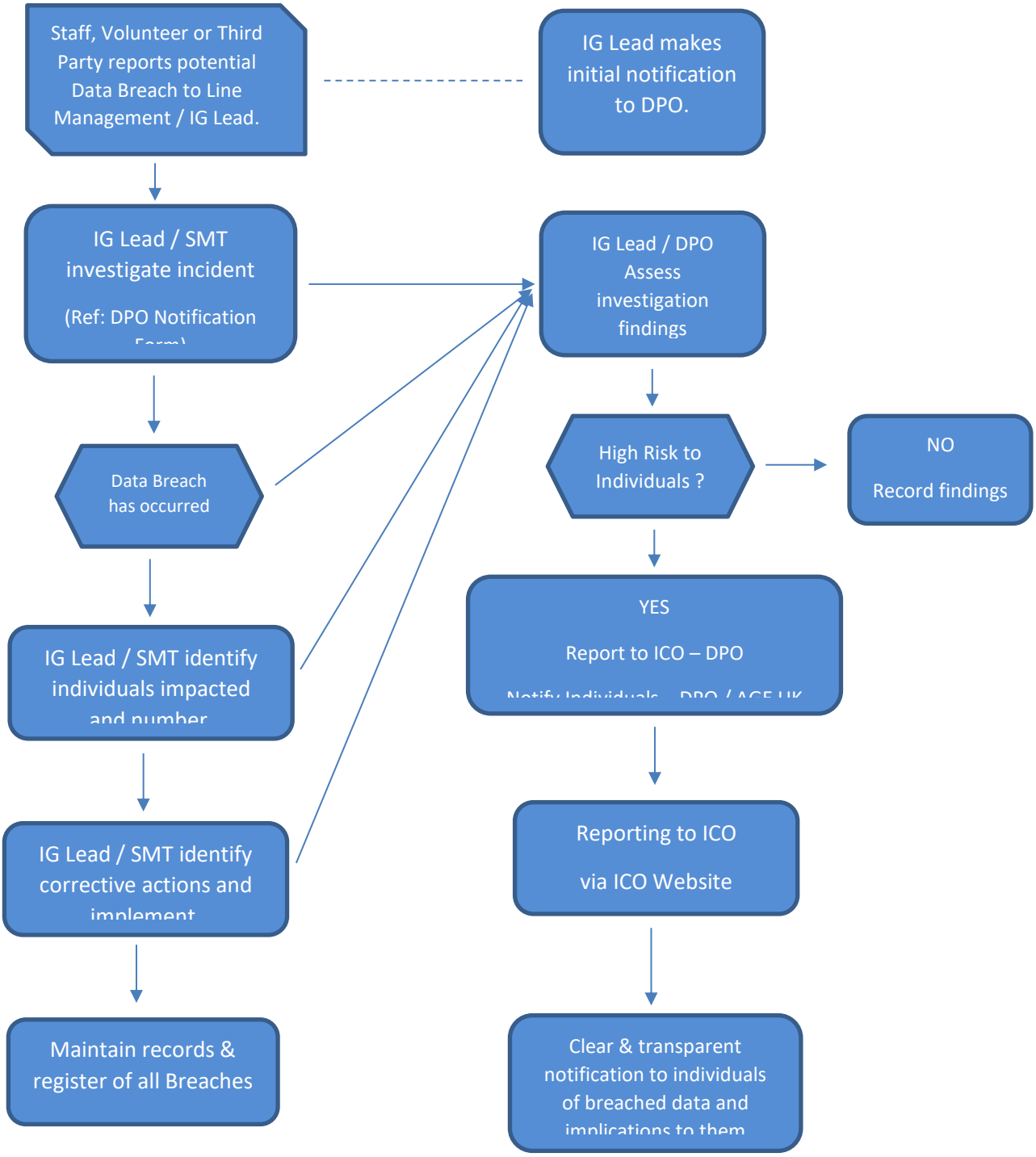
The Notification Form saved here: P:\Organisation & Governance\Data Protection & GDPR\Breaches\DPO Data Security Breach Reporting Form v1.2.docx requires details of the actions taken and can be used as a guide to the considerations which need to be made.

The flow chart below details the required process for dealing with a reported Data Breach incident.

The organisation shall maintain a register of all data security incidents which caused or had potential to cause a personal data breach. The DPO shall also maintain a record of incidents reported to them (Helpdesk records).

The register as a minimum shall detail the incident, and assigned corrective measures with completion dates, providing a means for senior management to monitor the status of corrective actions.

A5.9 Breach Response Flowchart



Appendix 6 - Change Management Policy

A6.1 Introduction and Scope

The Change Management / DPIA Policy and Procedure sets out the process for change and assessing the risk of any changes to personal data processing within Age UK STW. New processes will be managed and implemented in a way that shall minimise risk and impact to Age UK STW and its operations.

It is essential that changes to technology, business processes or loss or reduction of either, are assessed in terms of the potential impact on data processing and in particular the rights and freedoms of data subjects. In addition, new projects being proposed should have a formal approval process before the project is instigated.

The following process will be instigated and communicated throughout the organisation to ensure that any activities involving, or proposed changes to the processing of personal data shall be considered and documented in accordance with the UK GDPR.

A Change Management form / Data Protection Impact Assessment (DPIA) is required for all new/changes to business processing where there is potentially a high risk to the rights and freedoms of data subjects. However, a Risk Assessment is required for all processing of personal data. By completing the change management form the DPO will assess the information provided to determine whether a further DPIA or Risk Assessment is required. In some cases, where data is being transferred internationally, a Transfer Risk Assessment is required. The DPO will help the organisation complete this.

A6.2 Change Management Process

The Change Management process will follow a standard process for all requests for changes to an existing processing activity, or a new processing activity. The employee completing the Change Management form has overall responsibility for completing it. They will work with the DP Lead and DPO to complete the relevant assessment(s).

A6.3 Stage 1: Identification of Change to Processing of Personal Data

An employee identifies a need for a change to personal data processing, either implementing a new processing activity; sharing personal data with a new supplier; or a change to the processing activity, within the organisation and completes a Change Management Form with the support of the Employee completing it This form is sent to the DPO (Email) and DP lead along with any supporting documentation, such as vendor questionnaires and Data Processing Agreements. This should be done as early in the change lifecycle as possible and prior to

commencement of the processing to ensure adherence to GDPR requirements. The Change Management Form shall be wholly completed by the Lead employee, with support from the DP lead and the DPO.

A6.4 Stage 2: Assessment

The DP Lead and/or DPO will assess the Change Management Form and determine whether a further DPIA or Risk Assessment is required.

The DPO will work with the employee who completed the change management form and the DP Lead to complete any further risk or impact assessment. They will provide advice on whether the activity requires further measures to be put in place to protect the data or whether the activity should not go ahead. The DPO will then return this to the employee and DP Lead.

A6.5 Stage 3: Review and Implementation

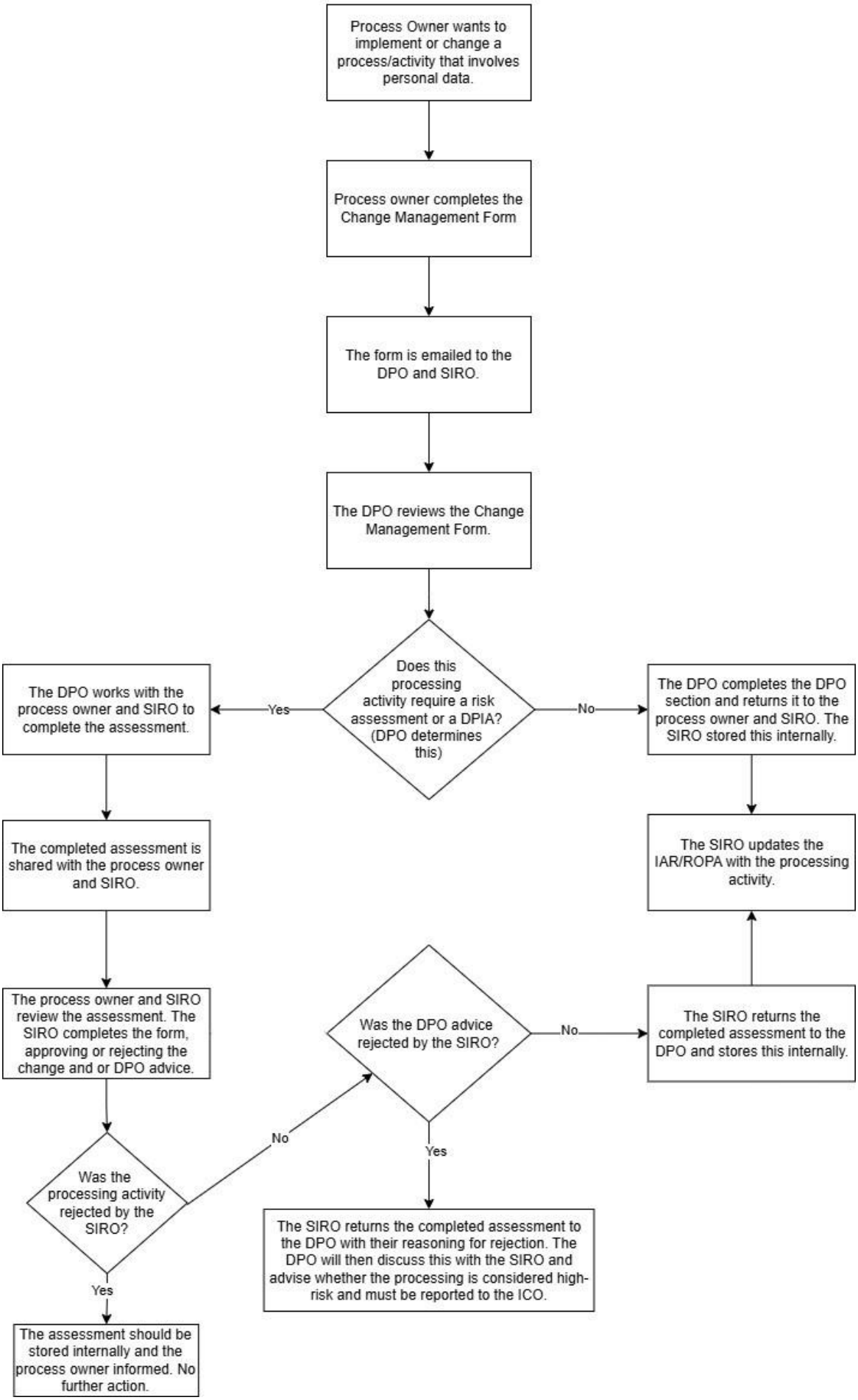
The Employee who has completed the Change Management form and DP Lead will review the DPO's assessment. The DP Lead will then complete the remainder of the form stating whether the change is approved and if the DPO advice is accepted. If the DPO's advice is rejected, the DPO will discuss with the DP Lead whether the activity requires reporting to the ICO due to its high risk.

The DP Lead will then store the change management form here:-

P:\Organisation & Governance\Data Protection & GDPR\Change Management - DPIA assessments

After this the DP Lead will implement the change with the Information Asset Owner. The information asset register and data retention schedule must then be updated with the new processing activity. The DP Lead can seek support from the DPO on how to update this if required.

A Change Management flow chart is below:


Process Owner wants to implement or change a process/activity that involves personal data.
Process owner completes the Change Management Form
The form is emailed to the DPO and SIRO.
The DPO reviews the Change Management Form.
Does this processing activity require a risk assessment or a DPIA? (DPO determines this)
Yes
No
The DPO works with the process owner and SIRO to complete the assessment.
The DPO completes the DPO section and returns it to the process owner and SIRO. The SIRO stored this internally.
The completed assessment is shared with the process owner and SIRO.
The SIRO updates the IAR/ROPA with the processing activity.
The process owner and SIRO review the assessment. The SIRO completes the form, approving or rejecting the change and or DPO advice.
Was the DPO advice rejected by the SIRO?
No
The SIRO returns the completed assessment to the DPO and stores this internally.
Was the processing activity rejected by the SIRO?
No
Yes
Yes
The SIRO returns the completed assessment to the DPO with their reasoning for rejection. The DPO will then discuss this with the SIRO and advise whether the processing is considered high-risk and must be reported to the ICO.
The assessment should be stored internally and the process owner informed. No further action.