Shropshire Telford & Wrekin Age UK

Data Protection & Security Policy

Updated April 22

Contents

1. Introduction

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

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

- Service clients

- Clients relatives / carers / Power of Attorneys
- Employees – current and past
- Volunteers
- Job applicants
- Donors & sponsors
- Staff of suppliers & partner organisations
- Members of public visiting our shops

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 – Chief Executive / DPO
- 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\Confidentiality Policy V6 Dec 20.docx

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 the DSAR Procedure:

Data Subject Access Request Procedure v2 April 22.docx

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 individual 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.

P:\Organisation & Governance\Data Protection & GDPR\Privacy Notices\Privacy Policy - Clients _ Supporters 2 - July 21 (1).docx

Whilst AGE UK STW does not rely solely on consent as the basis for lawful processing of personal data in all cases, it is policy to gain formal consent from all individuals, as part of its commitment to ensuring transparency and informed decisions by the individual.

Consent should be given in writing, although for some client 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 with their consent. (This includes photographs.), unless there is a legal requirement to do so.

All data subjects will be given the opportunity to opt out of their data being used in particular ways, such as the right to opt out of direct marketing (see below).

Age UK Shropshire Telford & Wrekin acknowledges that, once given, consent can be withdrawn, but not retrospectively.

There may be occasions where Age UK STW has a legal obligation to retain data for a certain length of time. Data retained will be kept to a minimum and should be anonymised wherever possible.

Consent shall be formally gained using the controlled consent form applicable to the data subject - client, employee or volunteer.
A specific Consent form is to be utilised for taking of and using client images (Photographs / Video)

P:\Organisation & Governance\Data Protection & GDPR\Consent Forms for upload\Consent Forms\Client Privacy Form v1 Oct 2021.pdf

9. Direct Marketing

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

Age UK Shropshire Telford & Wrekin will treat the following unsolicited direct communication with individuals as marketing:

- Seeking donations and other financial support.
- Promoting any Age UK STW services.
- Promoting Age UK STW events.
- Promoting membership to supporters.
- Promoting sponsored events and other fundraising exercises.
- Campaigning on behalf of older people
- Marketing on behalf of any other external company or voluntary organisation.
- Any of the above included in correspondence which is not marketing related.

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 assume that previous engagement with an individual provides 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.

Individuals can register a telephone number not to receive unsolicited marketing calls, ring 0845 070 0707 or visit www.tpsonline.org.uk

To register not to receive unwanted marketing mail, visit www.mpsonline.org.uk

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 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, which should be read alongside this policy.

P:\Organisation & Governance\Policies & Procedures\AUSTW.Policies\Policies under review\Electronic Communications & Social Media Policy V5 Dec 21 draft.docx

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 section below 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; which is also contained within this policy document.

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; be responsible for the investigation and handling of any such incidents.

Breaches\DPO Data Security Breach Reporting Form v1.2.docx

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 IG Lead.
Staff should also be aware of AGE UK STW Press & Media Contact procedure.

P:\Organisation & Governance\Policies & Procedures\AUSTW.Policies\Press & Media Contact Procedure V2 Jul21.docx

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, Acceptable Use 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.

14. Data Security Policy

Introduction & Scope

This 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 policy also include the measures to be applied by Staff or Volunteers working at home (Remote Working).

Responsibilities

The IG 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 IG 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 sign a Confidentiality Agreement.

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.

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.

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.

  P:\Organisation & Governance\Project, tenders and service development docs\Project docs\project docs & templates\Project Initiation Document V4 Nov 20.doc

- 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.

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.

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 hard copy data shall not be retained beyond its required use, if retention of the data held is required; it should be scanned and held electronically.

- All data which is being held to satisfy required retention purposes, shall only be held in electronic format, stored within the allocated share drive file and/or CRM, with access to it restricted.

- 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 shall 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 Policy, 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 and not by individuals at home.

- 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.

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
- 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 (Eg. 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. The use of personal equipment is not permitted.

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 periodically.

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.

Technical Measures

Senior management will ensure as a minimum, the following specific measures are implemented and maintained. These measures are mandatory requirements for the processing of any data held by AGE UK STW and apply to processing by both staff and volunteers.

It is the responsibility of both staff and volunteers to ensure compliance with these measures.

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 / Mobile Phones) 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 8 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 unique pin or fingerprint to access.
- 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.
- Hardcopy data secured when not in use – locked cabinets / drawers / cases
  (Including remote / Home Working)
- No documents shall be left in vehicles unattended / overnight.
- Hardcopies shredded following use – office shredder only, no Home shredding, all documents returned to office.
- 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 shall not be despatched by post.
- All transfers to Third Parties made under conditions of a Data Processing Agreement

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 10 & automatically security updated on connection.

- All staff and volunteers are subject to Acceptable User Policy (see below)

- 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.

- USB ports & CD drives shall be disabled on all PCs / Laptops.

- 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.

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

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.

15. Acceptable Use Policy

Introduction

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

Whilst Volunteers in most cases are not given access to the organisations E mail or IT systems, they should be aware of the following rules if they are given this access. All Volunteers should note the organisations rules regarding the use of Social media.

Most of our employees have access to electronic media and services, including computers, email, online services, the internet and the organisation's intranet. This 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
- Cyberbullying
- Social Media
- Remote Devices

It should be read in conjunction with the organisations data protection / security policies and the policies for bullying and harassment.

P:\Organisation & Governance\Policies & Procedures\AUSTW.Policies\Harassment and Bullying Policy.v5 June 18.docx

Electronic media 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 password protected files or encryption.

Managers must ensure that all new employees are made aware of this policy and procedure prior to using email and the internet. A definition of sensitive (Special Category Data) information is detailed in the Data Protection policy.

Email

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 email 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 lists for their own use and should be aware that this would be treated as a disciplinary matter and a data breach.

In line with the Data Protection Act information should not be stored for any longer than is necessary. E mail accounts should not be used for the storage of information that is needed to be retained. E mail accounts will be cleared of all retained messages on an annual basis.

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

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 and unreasonable 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.

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.

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. Unless essential 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.

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 the 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 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.

Social Media

The organisation recognizes and accepts that its employees or volunteers may keep personal blogs on their own internet sites and that internet social networking sites such as Facebook and Twitter are a useful way of interacting socially with colleagues and friends. In addition, the use of social media sites such as Twitter or Facebook 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 access to such sites 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 and volunteers 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 or volunteers 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 or volunteers must not make inappropriate reference to the organisation on a social networking or social media site to its employees, its customers, its suppliers.

Employees or volunteers 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 and volunteers 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 or volunteers from their home, or other personal computers, and irrespective of whether the posts are done during working hours or in their 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.

Remote Devices

Remote devices may include (the list is not exhaustive): smartphones, laptops, tablets, USB memory sticks, Flash drives.
Employees may be provided with a mobile telephone, a laptop or a tablet where it is deemed necessary in the course of their work. Staff should remember that this equipment remains the property of the charity and can be recalled at any time if required.

Mobile phones should be used purely for work-based calls. However, it is recognised that it may be useful for staff to use their 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 are likely to cause any damage to the equipment.

The purpose of this 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 & USB sticks) containing or accessing information must be approved prior to connecting to the network. This requires the approval of the person's line manager and the Director of Finance. An up to date list of all staff who have remote access will be kept by the Policy, Planning & Performance Manager.

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.