CONFIDENTIALITY, DATA & RECORD MANAGEMENT POLICY

1. INTRODUCTION

This policy sets out the organisations policy and systems in relation to the maintenance of confidentiality, data collection and sharing and the management of records. It should be read in conjunction with the Information Governance policy.

2. SCOPE

2.1 This policy applies to the personnel[1] of Age UK Blackburn with Darwen, the registered charity and its subsidiary.

2.2 This policy applies to the confidentiality of all employees, volunteers, potential employees and volunteers, ex-employees and volunteers, placements, secondees and trainees, service users, customers, donors, consultants, contractors and any other individual or organisation that has contact with the organisation directly or indirectly.

2.3 Any personnel may not during their association with the organisation, or after that relationship ceases, disclose to anyone other than where required by law, any information of a confidential nature relating to the organisation, or its business or customers. Please refer to the Information Governance Policy for further information.

All confidential records and documents, both electronic and paper, together with any copies or extracts thereof, made or acquired by personnel in the course of their role/association with the organisation, shall be the property of the organisation and must be returned to the organisation on the ceasing of that relationship.

During the course of their association with the organisation, personnel may become aware of personal or other confidential information, some of which may fall within the scope of current Data Protection regulations. Personnel will respect the confidentiality of all information, both during and subsequent to any role with the organisation.

3. PRINCIPLES

3.1 The organisation recognises the right of individuals to confidentiality and that they have a right to expect that personal details will be kept confidentially and in line with the requirements of law.

3.2 The organisation recognises that misuse of data can be damaging and distressing and is committed to the principles of UK Data Protection regulations and the organisation's Information Governance policy which provide individuals with protection from unwanted or harmful use of data.

[1] Personnel includes staff, volunteers, trainees, placements, secondees, consultants and contractors

3.3 The organisation believes that the right to privacy, confidentiality and appropriate use of data are essential to ensure all individuals have full confidence in the organisation and are treated with respect and dignity.

4. CONFIDENTIALITY

4.1.1 Policy

Confidentiality applies to all facts or information about an individual including, but not exclusively, personal and financial data and can also apply to expressed opinions.

4.1.2 Anyone disclosing personal data must ensure there is a legal and justifiable reason for disclosure of the data; that relevant consent is in place where required, and recorded; and positively confirm the identification of the individual receiving the data before disclosure. The legal basis for sharing information will be made clear to the data subject, at the point the information is collected.

4.2 Service users and customers

4.2.1 Explicit consent will be gained from all service users and customers for the organisation to collect and store information about them in order to be able to provide services, activities or actions related to the individual's service provision. Individuals will also be informed how long we will retain their data and for what purpose.

4.2.2 In situations where a service user is not able to provide consent due to reduced mental capacity and there is no-one with formal authorisation to act of their behalf, the best interests approach within the Mental Capacity Act will be followed and documented.

4.2.3 Facts and information about an individual will not be divulged or passed to a 3rd party without the individual's recorded consent (unless an exception applies – see below)

4.2.4 The fact that an individual has made contact with the organisation will not be divulged without their consent. This includes ensuring messages are not left on answerphones or with 3rd parties that could indicate this.

4.2.5 If the organisation is contacted by someone else on behalf of an individual, then we will only act on behalf of and/or share data with that individual's direct recorded permission or where there is a formal legal arrangement in place which allows for this, for example a Power of Attorney.

4.2.6 An individual's approach is treated as being to the organisation, rather than a specific worker. As such sharing information about individuals within the organisation, on a 'need to know' basis, is permitted under this policy.

4.2.7 Where consent is provided to share data for the purposes of service provision this will always be done using secure and confidential methods and as per the Transfer of Data Risk Assessment.

4.2.8 We will ask all service users and customers for consent to contact them in relation to our wider marketing activities, services and fundraising, and the methods by which we can contact them. Their response will be recorded and we will abide by this response.

4.3 Use of payment card devices

This policy covers the use of payment card devices which enable customers or donors to make payment by Debit or Credit card. Any service or activity which uses a payment card device must

comply with the Payment Card Industry Data Security Standard (PCI DSS) - compliance requirements and responsibilities of personnel are detailed in the organisation's financial procedures.

4.4 Complaints

Usually a complaint will be made by someone already known to the organisation and for whom we have consent to keep the relevant information, however this may not always be the case. In this instance consent to collect and store personal data for the purposes of investigating and communicating about the complaint will be requested and recorded. For all complaints the individual will be informed that the organisation will keep a record of the complaint and action taken, including any relevant personal information and for how long this will be retained. They will also be informed of their right to ask for this information to be destroyed.

4.5 Personnel

This section applies to current, ex and potential staff and volunteers, contractors, consultants, secondees, placements and trainees. The terms employee and volunteer should be taken to include all these roles.

4.5.1 Explicit consent will be gained from all individuals who apply to become an employee or volunteer with the organisation to collect and store data that is necessary to fulfil our obligations as part of the recruitment process as an employer and as an organisation that utilises volunteers. It is recognised that for some information the organisation has a legitimate interest to collect this information and consent is not required. In these instances individuals will be informed of the legal basis for collecting, utilising and sharing their data. Individuals will also be informed how long we will retain their data once they cease contact with the organisation and for what purpose.

4.5.2 When an individual is accepted by the organisation as an employee or volunteer explicit consent will be gained from the individual to collect, store and share data to fulfil our obligations as an employer and as an organisation that utilises volunteers and individuals will be informed who we will need to share their data with. It is recognised that for some information the organisation has a legitimate interest to collect this information and consent is not required. In these instances individuals will be informed of the legal basis for collecting, utilising and sharing their data. Individuals will also be informed how long we will retain their data once they leave the organisation and for what purpose.

4.6 Donors

When an individual makes a monetary or in kind donation to the organisation we will write to them to acknowledge this donation and to thank them. At this point we will also explain that the organisation will store their data for financial record keeping and audit purposes, inform them how long we will retain their data for, and of their right to ask for this data to be destroyed. We will also seek explicit consent to contact the individual again in the future about our activities and fundraising, and the methods by which we can contact them. Their response will be recorded and we will abide by this response.

4.7 Exceptions

It is recognised that there may be times when it is appropriate to breach confidentiality for legitimate reasons, without permission.

The reasons permitted under this policy are:

- If there is, or suspected to be, an immediate risk to life or a risk of serious harm

- When a safeguarding allegation or concern has been raised
- If the organisation has a legal obligation to disclose particular information
- If an allegation is made against the organisation that requires external investigation
- If there is a reason to believe the individual is withholding consent but does not have mental capacity to make an informed decision (following capacity check)

The decision to breach confidentiality in these circumstances may be taken by the Chief Executive or in their absence at least two senior managers collectively.

4.8 Requests for Access to Data

The organisation recognises an individual's right to request to see the information held about them through a Subject Access Request and has a process in place to respond to these appropriately and within the 30 day time limit.

The organisation also recognises that it may, in some circumstances, have obligations under the Freedom of Information Act to disclose data or information and will comply with these, taking the requirements of current Data Protection regulations into consideration

4.9 Breaches of Confidentiality

4.9.1 Instances of breaches of data protection and confidentiality should be recorded on an incident investigation form. These will be fully investigated and all corrective actions recorded. Where required breaches will be reported to the Information Commissioners Office and the data subjects of any lost data will be informed in line with the organisation's Loss of Data Response Plan.

4.9.2 All employees and volunteers will be made aware of this policy and of their right to invoke the Grievance Procedure if they believe information is divulged without their consent.

4.9.3 All other individuals will be made aware of this policy and of their right to invoke the Complaints procedure if they believe information is divulged without their consent.

4.9.4 The organisation takes allegations of a breach of this policy seriously and will follow the Disciplinary procedure to investigate and deal with such allegations.

4.9.5 Social Media

This policy covers the use of both organisational and personal social media by personnel. Confidential information about other personnel, customers and service users or organisational business should not be disclosed or posted on social media, without the explicit permission of the organisation and of the data subject. Personnel should take particular care when using social media that they do not break Data Protection regulations or breach this policy.

5. DATA COLLECTION AND RECORD MANAGEMENT

5.1 Policy

The organisation is committed to implementing the principles of UK Data Protection regulations in its processing of personal data:

- Personal data will be used for the purpose for which it was given
- Personal data will be collected and processed fairly and lawfully
- Data collected will be adequate, relevant and not excessive in relation to the purpose

- As far as practicable steps will be taken to ensure that data is accurate and where necessary, up to date
- Individuals will have a right of access to any records which relate to them personally, including any information from other parties
- Data shall not be kept for longer than is necessary for the purpose
- Technical and organisational measures will be taken against unauthorised or unlawful processing and against accidental loss, destruction or damage to data
- Where there is a legal basis for sharing information this will be done using secure methods in line with the organisations Data Transfer risk assessment

5.2 Data Retention and Storage

5.2.1 'Live' records either electronic or paper-based will be stored securely and access will be restricted to those who are, by necessity, authorised to see and process them. The organisations methods for ensuring security include:

- Use of locked drawers/filing cabinets with restricted key access
- Use of door locks and/or key pads
- Password protected access to our IT systems in a specified format
- Passwords are not shared
- Password protected access to the organisations database, along with different access levels to different types of data
- Intruder alarms and security systems on all our premises

5.2.2 Archived paper-based records will be stored securely at our Head Office using a key lock with restricted access to the key.
Electronic records will be clearly labelled as such either on our server or the organisations database.
All archived records will be clearly labelled as to what they are and the disposal date.
All archived records will be retrievable and identifiable using the labelling system.

5.3 Record Retention

The attached Record Retention Standards Document at Appendix A provides details of how long each type of record will be kept.

5.4 Disposal

5.4.1 The organisation will annually dispose of all relevant archived records in accordance with the Record Retention Standards.

5.4.2 A confidential waste disposal supplier will be used to dispose of all records which include personal or other confidential data, both regularly throughout the year and at the annual disposal

5.4.3 Manual shredders are also available for immediate destruction of information along with a confidential waste box and staff and volunteers are trained in disposal of confidential material.

5.4.4 An annual secure deletion process will be undertaken on our organisational database to remove records in line with the Record Retention document.

5.4.5 Hard Drive Disposal

Hard drives of obsolete PCs and other electronic devices such as photocopiers will be cleaned before being disposed of securely in accordance with WEE regulations.

5.5 DBS and Rehab of Offenders Act Information

The organisation recognises that it has particular responsibilities in relation to the processing of data related to DBS applications. With regard to DBS processing the organisation uses a third party umbrella body from which it does not receive or retain information related to content of DBS disclosures. The third party organisation provides us with the disclosure number and date of issue, which we retain for our records. We may ask the individual to give us sight of their disclosure but do not retain a copy. The organisation does collect wider information related to criminal convictions and the Rehabilitation of Offenders Act 1974 for potential staff and volunteers, in line with current regulations requesting if there are any unspent conditional cautions or convictions under the Rehabilitation of Offenders Act 1974; and any adult cautions (simple or conditional) or spent convictions that are not protected as defined by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (Amendment) (England and Wales) Order 2020. The content of these forms are saved securely with limited access.

5.6 3rd party data processors

The organisation has contracts in place with third party suppliers, which process data for which the organisation is the data controller. These include our CRM database provider, reporting platform provider and HR advice service. The organisation ensures that the supplier has relevant technical and organisational measures in place to protect the data and that these are reflected in the contract arrangements.

6. IMPLEMENTATION OF THE POLICY

6.1 Responsibilities of Management

6.1.1 The Chief Executive is the accountable person in relation to Information Governance. The operational lead is the Head of Prevention and Wellbeing. The senior management team are responsible for ensuring the correct and full implementation of this policy in their areas of activity. The senior management team is also responsible for ensuring that appropriate systems and resources are in place to enable its implementation.

6.1.2 Line/service managers are responsible for ensuring that their staff and volunteers adhere to this policy at all times and for ensuring its correct implementation.

6.2 Responsibilities of All Staff and Volunteers

All personnel are responsible for ensuring they understand the requirements of this policy and associated procedures and risk assessments, what it means to them in their role and for ensuring they abide by its requirements. They are also responsible for reporting any potential or actual breaches of this policy to their line manager, using the incident reporting system.

6.3 Induction and Training

6.3.1 All staff, volunteers, placements, secondees and consultants receive a copy of this policy at induction along with a discussion with their line manager to ensure understanding.

6.3.2 All staff and identified volunteers receive training guidance on the requirements of current Data Protection regulations and the organisation's Information Governance policy, along with any other specified training as required by the particular role. They also receive a copy of the Information Governance Handbook.

6.4 Audit

The organisation will carry out an annual audit of the application and understanding of the Confidentiality Policy, Information Governance Policy and procedures and the security access arrangements in all areas. The audit will follow a prescribed format.