



PRIVACY POLICY

KEY INFORMATION

Policy prepared, reviewed or amended by:	Suzanne Hilton - Chief Executive
Policy approved by Board of Trustees on:	22 May 2018
Policy became operational on:	25 May 2018 Reviewed February 2021
Next Review Date:	February 2024

For definition of terms used within this document, please refer to
Appendix 1 (Interpretation/Glossary of Terms Used)

1. Introduction

Age UK Bolton recognises that those involved in running a charity and delivering services will gain information about individuals and organisations during work activities. This can include clients, customers, suppliers, business contacts, employees, volunteers, contractors and other people we have a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the Charity's Data Protection and Confidentiality standards and to ensure compliance with the law.

This Privacy Policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, volunteers, customers/clients or suppliers, business contacts, contractors, website users or any other Data Subject.

Personal Data is any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone, or in combination with other identifiers that we possess, or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data, but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data specifically includes, but is not limited to:

- Names of individuals;
- Postal addresses;
- E-mail addresses;
- Telephone numbers;
- Recorded material, including filmed footage of individuals;
- Any other information relating to individuals, including information ascertainable from their appearance such as age, gender and ethnicity.

Sensitive Personal Data specifically includes, but is not limited to, information revealing: health or medical conditions, racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

In many cases, such information will not be stated as confidential, and individuals will have to exercise common sense and discretion in identifying whether information is expected to be confidential if not specifically stated as confidential when imparted, or not stated as confidential under this policy.

Age UK Bolton acknowledges the vital importance of confidentiality in the operation of its service and that a right to privacy is essential to ensure that the client has trust and confidence in the Organisation and is treated with respect and dignity.

2. Policy Statement

Age UK Bolton understands the importance of data privacy and confidentiality and owes a duty to its stakeholders to make data privacy and confidentiality policy a priority.

This Privacy Policy applies to all our personnel, including employees, trustees, volunteers, agency staff, job applicants, contractors and/or consultants. All personnel must read, understand and comply with this Privacy Policy when processing Personal Data on our behalf and attend training on its requirements. This Privacy Policy sets out what we expect in order for Age UK Bolton to comply with applicable law. Compliance with this Privacy Policy is mandatory. All employees are also bound by additional terms and conditions of confidentiality contained in their contract of employment.

This Privacy Policy (*together with Related Policies and Privacy Guidelines*) is an internal document and may not be shared with third parties, clients or regulators without prior authorisation from our Data Protection Officer (DPO).

3. Scope

Age UK Bolton recognises that the correct and lawful treatment of Personal Data will maintain confidence in the Organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The General Data Protection Regulations (GDPR) establishes a framework that will enable individuals to better control their personal data; harmonise rules and enforcement throughout the European Union (EU), and ensure data protection in a globalised world.

Age UK Bolton may potentially be exposed to fines of up to EUR 20 million (*approximately £18 million*) or 4% of total annual turnover - whichever is higher and depending on the breach - for failure to comply with the provisions of the GDPR.

All employees (permanent and temporary), trustees, volunteers, agency staff, job applicants, contractors and/or consultants are responsible for ensuring that personnel of Age UK Bolton (*and its subsidiary companies*) comply with this Privacy Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPO is responsible for overseeing this Privacy Policy and, as applicable, developing Related Policies and Privacy Guidelines. The DPO for Age UK Bolton is the Corporate Services Manager, located at Age UK Bolton, The Square, 53-55 Victoria Square, Bolton, BL1 1RZ.

Please contact the DPO if you have any questions about the operation of this Privacy Policy or the GDPR, or if you have any concerns that this Privacy Policy is not being, or has not been, followed. In particular, you must always contact the DPO in the following circumstances:

- (a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by Age UK Bolton);
- (b) if you need to rely on Consent and/or need to capture Explicit Consent
- (c) if you need to draft Privacy Notices or Fair Processing if you are unsure about the retention period for the Personal Data being Processed;
- (d) if you are unsure about what security, or other measures, you need to implement to protect Personal Data if there has been a Personal Data Breach;
- (e) if you are unsure on what basis to transfer Personal Data outside the European Economic Area (EEA) if you need any assistance dealing with any rights invoked by a Data Subject;
- (f) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a Data Privacy Impact Assessment (DPIA), or plan to use Personal Data for purposes, other than that for which it was collected;
- (g) If you plan to undertake any activities involving Automated Processing, including profiling or Automated Decision-Making. If you need help complying with applicable law when carrying out direct marketing activities;
- (h) if you need help with any contracts, or other areas, in relation to sharing Personal Data with third parties (including our vendors).

4. Why this policy exists

The purpose of this policy on Privacy and Confidentiality is:

- To comply with all data protection law and follow good practice
- To protect the rights and interests of staff, clients, volunteers and partners
- To provide transparency about how we store and process individuals' data
- To provide practical guidance and credibility to our Organisation and to instil confidence in it
- To comply with the General Data Protection Guidelines and other data protection legislation and effectively manage and minimise risks of a data breach.

5. Personal data protection principles

Age UK Bolton adheres to the principles relating to processing of Personal Data set out in the GDPR which require Personal Data to be:

- (a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency)

- (b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation)
- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation)
- (d) Accurate and, where necessary, kept up to date (Accuracy)
- (e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation)
- (f) Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality)
- (g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation)
- (h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests)

Age UK Bolton is responsible for, and must be able to demonstrate compliance with, the data protection principles listed above (Accountability).

6. Responsibilities

Everyone who works for or supplies services for and on behalf of Age UK Bolton has some responsibility for ensuring data is collected, stored and handled appropriately and processed, in line with this policy and data protection principles; however, the following people also have specific key areas of responsibility namely:

The **Board of Trustees** is ultimately responsible for ensuring that Age UK Bolton meets its legal obligations.

The **Data Protection Officer (DPO)** is responsible for:

- Keeping the Board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data Age UK Bolton holds about them (also called 'subject access requests')
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

The Age UK Bolton **Corporate Services Manager** is responsible for making sure that the IT Support Contractor ensures that:

- All systems, services and equipment used for storing data meet acceptable security standards
- Regular checks and scans are performed to ensure security hardware and software is functioning properly
- Any third-party services the Charity (or its subsidiary companies) is considering using to store or process data are evaluated; for instance, cloud computing services

The Age UK Bolton **Corporate Services Manager** is also responsible for making sure that the IT Support Contractor ensures:

- Approval of any data protection statements attached to communications, such as emails and letters
- Addressing of any data protection queries from journalists or media outlets like newspapers
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

7. Lawfulness, fairness, transparency

7.1 Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

Age UK Bolton may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows processing for specific purposes, some of which are set out below:

- the Data Subject has given his or her Consent;
- the processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests;
- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects: the purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices; or
- other GDPR acceptable processing grounds.

Age UK Bolton personnel, including employees, trustees, volunteers, agency staff, job applicants, contractors and/or consultants, must identify and document the legal ground being relied on for each processing activity (*in accordance with our guidelines on Lawful Basis for Processing Personal Data*).

7.2 Consent

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes, or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if it is intended to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless another legal basis of processing can be relied upon, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross-border data transfers. Usually, we will be relying on another legal basis (and not require Explicit Consent) to process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents, so that Age UK Bolton can demonstrate compliance with Consent requirements.

7.3 Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices, which must be concise, transparent, intelligible, easily accessible and in clear and plain language, so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources, employment purposes or service delivery, we must provide the Data Subject with all the information required by the GDPR, including the identity of the Data Controller and DPO, how and why we will use, process, disclose, protect and retain that Personal Data through a Fair Processing Notice, which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (*for example, from a third party or publicly available source*), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check

that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

You must comply with the Age UK Bolton guidelines on drafting Privacy Notices / Fair Processing Notices.

8. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained, unless you have informed the Data Subject of the new purposes and they have, where necessary, Consented.

9. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only process Personal Data when performing your job duties so require it. You **may not** process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties; **do not collect excessive data**. Ensure that any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that, when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Age UK Bolton data retention guidelines.

10. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which

we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.

Age UK Bolton will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. **(You must comply with the Charity's guidelines on Data Retention.)**

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Age UK Bolton applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

12. Security integrity and confidentiality

12.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Age UK Bolton will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data. You are responsible for protecting the Personal Data that we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- (i) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

- (j) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- (k) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our Privacy Policy and (together with Related Policies and Privacy Guidelines) **OR** comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

12.2 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

Age UK Bolton has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches (the DPO or Chief Executive). You should preserve all evidence relating to the potential Personal Data Breach.

13. Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- the European Commission has issued a decision confirming that the country to which the Personal Data is transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- appropriate safeguards are in place, such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the GDPR, including the performance of a contract between us and the Data Subject; reasons of public

interest; to establish, exercise or defend legal claims, or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and, in some limited cases, for our legitimate interest.

14. Data Subjects' rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to processing at any time;
- receive certain information about the Data Controller's processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed, or to rectify inaccurate data or to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling (ADM);
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed above **(do not allow third parties to persuade you into disclosing Personal Data without proper authorisation)**.

You must immediately forward any Data Subject request you receive to your supervisor or the DPO and comply with the Age UK Bolton Data Subject response process.

15. Accountability

The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Age UK Bolton is required to have adequate resources and controls in place to ensure and to document GDPR compliance including:

- appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
- implementing Privacy by Design when processing Personal Data and completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents, including this Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;
- regularly training personnel on the GDPR, this Privacy Standard, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches; the Company must maintain a record of training attendance by Company Personnel; and
- regularly test the privacy measures implemented and conduct periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

16. Record keeping

The GDPR requires that Age UK Bolton keeps full and accurate records of all our data processing activities.

You must keep and maintain accurate corporate records reflecting our processing, including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with our record-keeping guidelines.

These records should include, as a minimum, the name and contact details of the Data Controller and the DPO; clear descriptions of the Personal Data types; Data Subject types; Processing activities; Processing purposes; third-party recipients of the Personal Data; Personal Data storage locations; Personal Data transfers; the Personal Data's retention period; and a description of the security measures in place. In order to create such records, data maps should be created, which should include the detail set out above together with appropriate data flows.

17. Training and audit

Age UK Bolton is required to ensure that all personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training, and ensure your team undergo similar mandatory training in accordance with our mandatory training guidelines.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18. Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when processing Personal Data, by implementing appropriate technical and organisational measures (*like Pseudonymisation*) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs / systems / processes that process Personal Data, by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

Data controllers must also conduct DPIAs in respect to high risk processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- large scale processing of Sensitive Data; and
- large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;

- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

You must comply with the guidelines on DPIA and Privacy by Design.

19. Automated Processing (including profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

- a Data Subject has Explicitly Consented;
- the processing is authorised by law; or
- the processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed, but such Sensitive Data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest, like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed, when you first communicate with them, of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

Age UK Bolton is required also to inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences, and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

Where you are involved in any data processing activity that involves profiling or ADM, you must comply with the guidelines on profiling or ADM.

20. Direct marketing

Age UK Bolton is subject to certain rules and privacy laws when marketing to our clients / customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers, known as 'soft opt in', allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar

products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner, so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

You must comply with the guidelines on direct marketing to customers.

21. Sharing Personal Data

Generally, Age UK Bolton is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of Age UK Bolton (or our subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a fully executed written contract that contains GDPR approved third party clauses has been obtained.

You must comply with the guidelines on sharing data with third parties.

22. Changes to this Privacy Policy

Age UK Bolton reserves the right to change this Privacy Policy at any time without notice to you, so please check back regularly to obtain the latest copy of this Privacy Policy. We last revised this Privacy Policy on 22nd May 2018.

23. Acknowledgement of receipt and review

I, _____[EMPLOYEE NAME], acknowledge that on
_____[DATE], I received and read a copy of the Age UK Bolton
Privacy policy dated and understand that I am responsible for knowing and abiding by its
terms. I understand that the information in this Privacy Policy is intended to help Age UK
Bolton work together effectively on assigned job responsibilities and assist in the use and
protection of Personal Data. This Privacy Policy does not set terms or conditions of
employment or form part of an employment contract.

Signed:

Printed Name:

Date:

APPENDIX 1

Interpretation/Glossary of Terms Used

Definitions:

Age UK Bolton: means the registered charity Age UK Bolton (Reg. No. 223240) and any/all of its subsidiary companies.

The words “**we**”, “**us**”, “**our**” and “**the Charity**”, as used in this document, refer to Age UK Bolton and its subsidiary companies.

The term “**you**” and “**your**”, as used in this document, refer to any / all personnel of Age UK Bolton and its subsidiary companies.

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Client / Customer: anyone who uses the service directly or indirectly, whether this be an older person, their representative or carer, or another organisation.

Charity Personnel / Personnel: all employees (permanent or temporary), trustees, volunteers, agency staff, contractors and/or consultants working for or supplying services to Age UK Bolton or its subsidiaries.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject’s wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers that we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (*for example, a name, email address, location or date of birth*) or an opinion about that person's actions or behaviour.

Personal Data specifically includes, but is not limited to:

- Names of individuals;
- Postal addresses;
- E-mail addresses;
- Telephone numbers;
- Recorded material, including filmed footage of individuals;
- Any other information relating to individuals, including information ascertainable from their appearance such as age, gender and ethnicity.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Personnel: *see Charity Personnel above.*

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Guidelines: the Company privacy / GDPR related guidelines provided to assist in interpreting and implementing this Privacy Policy and Related Policies, available here: **[Privacy Notices (also referred to as Fair Processing Notices)]**: separate notices setting out information that may be provided to Data Subjects when we collect information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (*for example, employee privacy notices or the website privacy policy*) or they may be stand-alone, one-time privacy statements covering processing related to a specific service or purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information, which is meant to be kept separately and secure.

Related Policies: the policies, operating procedures or processes related to this Privacy Policy and designed to protect Personal Data.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.