

Basic Information			
Document Owner		D Moran	
Approver		Board of Trustees	
Review Cycle		Annually	
Responsible Function			
Version Control			
Version	Date	Author	Reason for Update
2	04/12/25	D Moran	Cycle review

CONFIDENTIALITY & DATA PROTECTION POLICY (GDPR)

Introduction

The GDPR (General Data Protection Regulations) came into force in May 2018. Age UK Buckinghamshire has updated its confidentiality & data protection policy for staff & volunteers in line with this change.

Age UK Buckinghamshire staff and volunteers are expected to follow this policy, along with other data protection guidance.

Age UK Buckinghamshire is a data controller. The Chief Executive Officer has overall responsibility for data protection within the organisation.

As a data controller, Age UK Buckinghamshire is expected to comply with the principles of good information handling:

1. Process personal data **fairly, lawfully and in a transparent manner**.
2. Obtain personal data only for one or more **specified and lawful purposes** and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is **adequate, relevant and not excessive** for the purpose or purposes for which it is held.
4. Ensure that personal data is **accurate** and, where necessary, **kept up to date**.
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.

Individuals (data subjects) have the following rights:

- Personal and special categories of personal data cannot be held without lawful basis (however, the consequences of not holding it can be explained and a service withheld).
- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.
- Individuals have a right to have their data erased and to prevent processing in specific circumstances:

- Where data is no longer necessary in relation to the purpose for which it was originally collected
 - When an individual withdraws consent
 - When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
 - Personal data was unlawfully processed
- An individual has a right to restrict processing – where processing is restricted, Age UK Buckinghamshire is permitted to store the personal data but not further process it.
 - An individual has a 'right to be forgotten'.
 - An individual can ask to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (Age UK Buckinghamshire) must comply with such requests within 30 days of receipt of the written request.

Lawful basis & consent

The GDPR regulations set out the lawful basis for holding personal information. **If Age UK Buckinghamshire holds any personal / identifiable information we must have a lawful basis for doing so.** One of the following must apply:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

(g) Special Category Data: the processing of Special Category Data to deliver services, support beneficiaries, manage volunteers and staff, or carry out research and advocacy. This type of data requires a valid lawful basis under the UK GDPR, and where an additional condition for processing Special Category Data is met.

In most cases, there is a requirement for **explicit consent** from the individual to process their Special Category Data.

At Age UK Buckinghamshire, the lawful basis for holding information and how we will record this is as follows:

Use of data	Lawful basis for holding	How we will gather and record
Store on database	Special Category Data	Gathered via consent form or verbally and stored on Charity log.
Sharing of information	Consent	Gathered via consent form or verbally and stored on Charity log.
Marketing Communications (Email, post, phone)	Consent	Gathered via consent form or verbally and stored on Charity log.

Sharing of information- clients must be informed exactly who we will share their information with.

Consent for publicity must also be sought.

Staff & volunteer guidance on the procedure for storing consent is available separately.

Withdrawing consent - People have the right to withdraw consent at any time.

Ensuring the security of personal information

How we hold & share data

- Age UK Buckinghamshire hold data within our secure Office 365 cloud server. Any personal information is then kept in another secure server Charity Log. AUKB do not share your data unless we have consent to do so. Data is only shared without consent should there be a safeguarding issue.
- Age UK Buckinghamshire hold data protection spot checks on all staff members to ensure staff are following the policies and guidance.
- Staff systems can be monitored by Senior Management should there be need for this.
- For safety reasons and to have heightened security of data breaches, Age UK Buckinghamshire do not allow any staff member to insert any removable devices (i.e., memory sticks/cards/CD's) to their laptops.

Paper Records

- In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working the day. If your work involves you having personal /

and/or special categories of personal data at home or in your car, the same care needs to be taken.

- Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.
- If you are transferring papers from your home, or your client's home, to the office for shredding this should be done as soon as possible and not left in a car for a period of time. When transporting documents, they should be carried out of sight in the boot of your car.
- Paper records should not be held longer than necessary (see retention of records)
- Any record that can be held electronically and not in paper form should be.
- Finance paper records are to be placed in lockable filing cabinets and confidentiality shredded after 7 years. We are to receive a certificate of confirming for the shredding.

Electronic Records

- All information must be held on the secure Age UK Buckinghamshire systems.
- Passwords and a system of limited access must apply to all information held on the server.
- Protection such as firewalls and other internet security should be in place at all times and reviewed by I.T. support.
- Confidential information sent out by email must be encrypted, password protected or if possible, sent in a way that does not allow the information to be used if intercepted by i.e., by splitting up content.
- Confidential information should only be sent out by email when essential and that information should be kept to a minimum.
- Confidential information held electronically must not be held longer than necessary (see retention of records)

Charitylog

Charitylog, hosted by Dizions Ltd, holds data about our service users, volunteers and staff. Access is password protected and restricted to named users, with level of access to each user on a 'need to know' basis to be able to carry out their job. Charitylog is accredited to ISO 27001:2013 Information Security standard. They are also accredited to the International

Quality Management Standard ISO 9001:2008 and are registered with the Information Commissioners Office. Charitylog is also signed up to Cyber Plus Essentials. As such Age UK Buckinghamshire is satisfied with the security levels in place to protect its data.

Staff & Volunteer Personal Data

- Each staff member/volunteer working for Age UK Buckinghamshire will have a personal file containing confidential information. Personal records should be kept in either a locked cabinet and/or secure server storage. Access to these files will be by the Chief Executive and Senior Management and where appropriate, trustees in the case of staff members. Should information contained in these files come to light by means of accident or any other way, to anyone other than the appropriate supervisor or employee/volunteer themselves, then such information should not be divulged to a colleague, volunteer or other third party within or outside the organisation.
- Each individual staff member/volunteer will have the choice as to whether they wish their telephone number and/or address, or any other personal details, to be divulged to any other person either inside or outside the organisation, other than to be kept as a record (hard copy or e-version) for personnel purposes within their personal file. No such details will be given without active consent.
- Personal details pertaining to Board members may also be kept on record (hard copy or e-version) within the organisation. Any other personal information, other than that mentioned, pertaining to Board members shall not be divulged either within or outside the organisation, other than with that individual's consent and as advised by the Chief Executive Officer.
- For staff and volunteers who are regularly involved with vulnerable adults, it may be necessary for Age UK Buckinghamshire to apply to the Disclosure & Barring Service to request a disclosure of spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to specific managers. If there is a positive disclosure this will be reviewed by senior management in line with our DBS policy to assess the risk of appointment.

Client personal data

- Clients' details should not be disclosed or discussed with anyone outside the organisation in such a manner that it is possible to identify the client, unless the client agrees to such information being passed on to a third party. An enquirer's approach is to the organisation rather than to an individual employee or volunteer. Therefore, if the needs of a particular client are best served by discussion with another staff member/volunteer, then such disclosure does not breach the policy. If,

however, a client specifically requests that information is not divulged to a third party of any kind, then this wish should normally be respected.

- The situation often arises when an enquiry is made on behalf of someone else (third party), e.g., by a relative; friend or neighbour, and in these circumstances, it is allowed to give general advice or information to the enquirer. However, should a specific request be made for help or assistance that would necessitate Age UK Buckinghamshire referring the potential client to a third party, or Age UK Buckinghamshire visiting that person, then a request must be made by the persons themselves for such assistance either verbally or in writing. If the individual concerned is not in fit state mentally or physically to give such permission, it should be sought by their carer, next of kin or advocate, as may be appropriate in the circumstances. If a staff member/volunteer is in any doubt whatsoever about the validity of the third-party enquiry, they should consult with the Chief Executive Officer, or member of staff with authority to deputise.
- Records and files relating to service users are available to staff and volunteers who have signed the statement on confidentiality. Care must be taken at all times to ensure that all records/files are handled with discretion and are not left around on desks or in public view. The same principles should be applied with confidential information in memos, e-communications, letters, briefing papers and minutes of meetings. When client records are not in use, and when the office is unmanned, the records should be kept in locked cabinets.
- The same principles of confidentiality shall apply to all clients, whether they are being dealt with in person, by correspondence, by e-communication or by telephone.
- If it is necessary for staff/volunteers to remove confidential information regarding clients from the premises, e.g., on home visits or to attend meetings, due care and attention must be exercised to ensure that such material is kept safely in their possession at all times. Particular care should be taken with personal diaries or laptops which may contain details of service users such as names and addresses. No such material/information should be left unattended.
- Client information must not be kept on file any longer than is reasonably necessary.
- Data Subject Access Request (SAR)- Age UK Buckinghamshire will comply with any SAR requests that are made, at no charge to the individual making the request. The Chief Executive Officer is responsible for ensuring that the request is fulfilled within 30 days.
- A Privacy Notice is kept updated and made available via the website or on request.

Organisational confidential information

- Staff and volunteers may receive confidential or sensitive information relating to Age UK Buckinghamshire or other organisations. The same standards of confidentiality should be adhered to as is the case with client's information been dealt with at Age UK Buckinghamshire. Such information should only be divulged to a colleague or third party within the organisation, and never to anyone outside without consultation with senior management.
- Any confidential or sensitive matters pertaining to any aspect of work of Age UK Buckinghamshire, its staff, volunteers or Board members should not in any circumstances be discussed with any third party outside the organisation, without prior discussion with the Chief Executive Officer. Nor should such information be discussed with a third party within the organisation without prior consultation with the person it concerns or senior management, whichever would be the most appropriate, depending on the nature of the information (e.g., personal or organisational).
- Board Members shall be expected to comply with the same standards of confidentiality specified in this policy at all general and special meetings of the organisation. Specifically, in respect of any confidential agenda items, Board members will be expected to adhere to the policy and guard against any breaches either intentional or unintentional.
- Any staff members, volunteers or staff representatives attending meetings must also comply with the standards of confidentiality as set out in this policy and guard against any breaches either intentional or unintentional.
- Any minutes produced as a result of such meetings shall not be divulged to a third party outside the organisation, without prior consultation with the Chief Executive Officer. Any minutes that exist of any confidential agenda items, particularly pertaining to named individuals, should not be disclosed to any person or third party excluded from discussion of such agenda items, either inside or outside the organisation, unless specifically authorised by the Chief Executive Officer or Chairperson of any such meetings, as may be appropriate.

Retention of records

It is Age UK Buckinghamshire's policy to not hold records any longer than they are needed. Records will be kept for the following timeframes:

- Client records – 6 years after ceasing to be a client. Longer should Age UK Buckinghamshire have a 'Legitimate Interest' to do so.
- Staff records – 6 years after ceasing to be a member of staff.
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Volunteer records – 6 years after ceasing to be a volunteer.
- Timesheets and other financial documents – 7 years.

- Other documentation, e.g., client plan sent to a worker as briefing for a visit, should be destroyed as soon as it is no longer needed for the task in hand.

Paper records should be destroyed after the above timeframes have ended. Computerised records e.g., Charitylog, to be anonymised six years after ceasing to have any services from us. (Anonymising will remove the personal and special categories of personal data but will not remove the statistical data.)

We retain data for six years because the limitation period for many civil actions is six years from the date of the cause of action arising.

Confidentiality or data protection breach

Use of public Wi-Fi (e.g., Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data. Staff, directors, trustees and volunteers are advised to not use this to connect to our systems.

On occasion staff members take paperwork out of the office. If this happens, they are to be kept in a secure place. Staff are not to leave papers in their cars overnight and keep out of sight from the public.

When people change roles or leave our organisation, there needs to be a reliable way to amend or remove their access to our IT system(s). It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses. Although we change access when needed to ensure this is done properly, we hold a periodic audit to make sure that people's access rights are at the right level. At the same time all passwords for systems, Wi-Fi and emails are changed.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

- Personal data breaches can include:
- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

If you discover, or suspect, a data protection breach you should report this to your line manager who will review our systems, in conjunction with the Senior Management Team, to prevent a reoccurrence. Senior Management should investigate the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and also for reporting to the Board of Trustees. There is a time limit for reporting breaches to ICO so Senior Management should be informed without delay.

The Chief Executive is responsible for reporting data breaches to the ICO. Not all breaches need to be reported, however. <https://ico.org.uk/for-organisations/report-a-breach/>

Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action which may result in dismissal.

Data Protection Impact Assessment (DPIA)

Age UK Buckinghamshire is aware of the need to complete a DPIA for new or substantial changes to projects involving the use of personal data that are likely to result in high risk to individuals' data.

We consider whether to do a DPIA if we plan to carry out any other:

- evaluation or scoring
- automated decision-making with significant effects
- systematic monitoring
- processing of sensitive data or data of a highly personal nature
- processing on a large scale processing of data concerning vulnerable data subjects
- innovative technological or organisational solutions
- processing that involves preventing data subjects from exercising a right or using a service or contract

We always carry out a DPIA if we plan to:

- use systematic and extensive profiling or automated decision-making to make significant decisions about people
- process special-category data or criminal-offence data on a large scale
- systematically monitor a publicly accessible place on a large scale
- use innovative technology in combination with any of the criteria in the European guidelines

- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit
- carry out profiling on a large scale
- process biometric or genetic data in combination with any of the criteria in the European guidelines
- combine, compare or match data from multiple sources
- process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines
- process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them
- process personal data that could result in a risk of physical harm in the event of a security breach

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.