**AGE UK**

**NORTH CUMBRIA**

**Confidentiality Policy**

**Adopted: May 2018**

**Reviewed: Jan 2025**

**Next Review: Jan 2026**

**Reg Charity No 1128565**

**A blue and white logo

Description automatically generated**

**Confidentiality Policy**

1. **Introduction**

* 1. Age UK North Cumbria is responsible for managing personal data about The Organisation, its Employees, Trustees, Volunteers, Clients, and any other individual involved in the Organisation to enable it to carry out its day-to-day business. All personal data will be dealt with sensitively and in the strictest confidence.
  2. For the purpose of this policy, confidentiality relates to the transmission of personal, sensitive, or identifiable information about any Individual or Organisation, which comes into the possession of Age UK North Cumbria through its work.
  3. This Policy applies to all Age UK North Cumbria activities and is adopted by Employees, Trustees, Volunteers, and any other Individual involved with the Organisation.
  4. Age UK North Cumbria will adhere to the principles and procedures contained within UK legislation and guidance. Taking the following particularly into consideration:
* [The Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted)
* [The Human Rights Act 1998](https://www.legislation.gov.uk/ukpga/1998/42/contents)
* [The Care Act 2014](https://www.legislation.gov.uk/ukpga/2014/23/contents/enacted)
* [The Children Act 1989](https://www.legislation.gov.uk/ukpga/1989/41/contents)
* [The Children Act 2004](https://www.legislation.gov.uk/ukpga/2004/31/contents)
* [The Caldicott Review 1997, 2013 and 2016](https://www.gov.uk/government/publications/the-caldicott-principles)

1. **Purpose**

# The purpose of the Confidentiality Policy is to ensure that all Employees, Trustees, Volunteers, Clients, and any other Individual involved in the Organisation understand the Organisations’ requirements in relation to the disclosure of personal data and confidential information.

1. **Principles** 
   1. Age UK North Cumbria is committed to providing a confidential service for all; therefore, the below principles should always be adhered to in relation to personal data:

* Maintain justifiable reasons for collecting and retaining confidential data.
* Only use the data for the purpose for which it was gathered and where it is necessary.
* The minimum amount of personal confidential data transferred or accessible, as is necessary for a given function to be carried out.
* Inform Individuals about how their confidential data is used and what choices they have around this (Data Protection Privacy Notice, Appendix 1).
* Only those who need access to personal confidential data will have access to it.
* Everyone with access to personal data is aware of their responsibilities in relation to confidentiality.
* No confidential data given to the Organisation will be shared with any third party, without that Individual’s or Organisation’s expressed permission (verbal or written), unless required by law.
* Where an Individual is unable to provide meaningful consent to share data, then this must be sought from an Individual’s named legal representative (evidence required).
* It is acknowledged that there may be occasions where it is in the Best Interests of an Individual to share confidential data, and these should be discussed directly with a Line Manager and Chief Executive Officer prior to any disclosure being made.
* Any unauthorised disclosure of information (verbal, written or implied) will be treated as a very serious matter.

**4. Responsibilities**

4.1 The Chief Executive Officer (CEO) has overall responsibility for ensuring the

effective implementation of Age UK North Cumbria’s Confidentiality Policy and this is supported

on a day-to-day basis by all Employees, Trustees, Volunteers, and any other Individual involved

with the Organisation adopting and endorsing these.

1. **Action to be taken**
   1. All Employees, Trustees, Volunteers, and any other Individual involved in the Organisation will receive a copy of the Confidentiality Policy, as part of their induction and training. Line Managers must ensure that the Confidentiality Policy Statement (Appendix 2) is completed at the first viable opportunity.
   2. All personal paper-based and electronic data must be stored in accordance with The Data Protection Act (2018) and The Retention, Destruction and Disposal Policy. They must be secured against unauthorised access, accidental disclosure, loss, or destruction.

* 1. All personal paper-based and electronic data must only be accessible to those individuals authorised to have access. This includes Employees, Trustees, Volunteers, and any other Individual involved in the Organisation identified through stringent recruitment processes (see Recruitment and Selection Policy), received appropriate training, and clearly understand their responsibilities around confidentiality.
  2. All paper enquiry records should be kept in lockable cabinets if they cannot be transferred on to Compass or other organisational databases, with access limited to relevant staff. (see Retention, Destruction and Disposal Policy).
  3. Electronic records and files should be regularly monitored, and information destroyed when it is no longer necessary to keep it. Any paper records and files containing confidential data should, when no longer needed, be shredded (see Retention, Destruction and Disposal Policy).
  4. It is sometimes necessary for Employees, Trustees, Volunteers and any other Individual involved in the Organisation to carry information relating to Clients with them on home visits or when attending meetings or case conferences. It is expected that they exercise due care and attention to ensure that such material is kept to a minimum, is safe, and in their possession at all times. Particular care should be taken with diaries and other documentation where appointments indicate the name and address of a Client. No such material/information should be left unattended in a vehicle. Papers should be returned to the office as soon as possible and always before the end of the working day.
  5. Any electronic device used in community work should be password protected and stored securely. The includes smartphones, tablets, laptops, and USB or other external storage devices.
  6. Employees, Trustees, Volunteers, and any other Individual involved in the Organisation can share personal information with their Line Manager to discuss issues and seek advice appropriately.
  7. It is also acknowledged as part of learning and development processes, there may be occasions when Employees, Volunteers, and any other Individual involved in the Organisation wish to discuss a case to gain a wider perspective on the bast ways to approach this. However, any information considered identifiable should always be avoided.
  8. The Organisation recognises their responsibility to share confidential information in line with the Legislation and includes the following specific circumstances –
* Where there is risk of danger to an Individual.
* If it is in the public interest to do so, although steps should be taken to gain consent, if it is safe.
* Where it is against the law to withhold it. In these circumstances, information may be divulged to external agencies e.g., police or social services on a need-to-know basis.

All occasions of breaches of confidentiality without consent must be discussed with the Chief Executive Officer.

* 1. If an Employee, Trustee, Volunteer, and any other Individual involved in the Organisation feels confidentiality should be breached outside of these circumstances the following steps will be taken: They should raise the matter immediately with their Line Manager, discussing the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved by breaching confidentiality. The Line Manager should take a written note of this discussion. The Line Manager is responsible for discussing what options are available in each set of circumstances. The Line Manager is responsible for deciding whether confidentiality should be breached. If the Line Manager decides that confidentiality is to be breached, then they should take the following steps: The Line Manager should contact the Chief Executive Officer (CEO), giving an accurate account of the full facts of the case to seek authorisation to breach confidentiality, ensuring they do not breach confidentiality in doing so. If the CEO agrees to breach confidentiality, a full written report on the case should be made and any action agreed undertaken. The Line Manager is responsible for ensuring all activities are actioned. If the CEO does not agree to breach confidentiality, then this decision is final.
  2. All Employees, Trustees, Volunteers, and any other Individual involved in the Organisation should avoid exchanging personal information or making comments about Individuals or Organisations with whom they have a professional relationship with, during both working hours and social settings.
  3. If an Employee, Volunteer, Trustee, or any other Individual involved in the Organisation accesses another’s personnel records, without authority, then the Disciplinary Policy and Procedure will be invoked.
  4. All Employees, Volunteers, Trustees, and any other Individual involved in the Organisation hold the right to inform their Line Manager or a Trustee if they believe that Age UK North Cumbriais being brought into disrepute by the actions of another, even if doing so could breach confidentiality (see Whistleblowing Policy).
  5. Breaches of this Policy will be dealt with under the Disciplinary Policy and Procedure, as appropriate.
  6. Employees, Volunteers, Trustees, and any other Individual involved in the Organisation can be criminally liable if they knowingly or recklessly disclose personal data in breach of the Date Protection Act (2018).

# **6. Recording**

6.1 All personal data should be recorded in line with The Data Protection Act (2018) and the Retention, Destruction and Disposal Policy.

6.2 The Organisation is committed to effective statistical recording of the use of its services to monitor usage and performance and develop its services in line with demand and need. All statistical records given to third parties, such as to support funding applications or project monitoring reports shall be produced in anonymous format, so individuals cannot be recognised. Consent processes will also cover participation in statistical reporting.

**7. Monitoring and Review**

7.1 The implementation and effectiveness of this Policy will be monitored, reviewed (no less than annually) and updated to remain compliant with current Legislation and guidance by the CEO.

**Appendix 1**

**Age UK North Cumbria**

**Data protection privacy notice (employment)**

This notice explains what personal data (information) we hold about you, how we collect it, and how we use and may share information about you during your employment and after it ends. We are required to notify you of this information under data protection legislation. Please ensure that you read this notice (sometimes referred to as a ‘privacy notice’) and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

**Who collects the information**

Age UK North Cumbria is a ‘data controller’ and gathers and uses certain information about you and so, in this notice, references to ‘we’ or ‘us’ mean the Company.

**Data protection principles**

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

**About the information we collect and hold**

**What information**

We may collect the following information during your employment:

Your name, contact details (ie address, home and mobile phone numbers, email address) and emergency contacts (ie name, relationship and home and mobile phone numbers);

Information collected during the recruitment process that we retain during your employment;

Employment contract information;

Details of salary and benefits, bank/building society, National Insurance and tax information, your age;

Details of your spouse/partner and any dependants;

Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;

A copy of your driving licence;

Details of your pension arrangements, and all information included in these and necessary to implement and administer them;

Information in your sickness and absence records (including sensitive personal information regarding your physical and/or mental health);

Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs;

Criminal records information, including the results of Disclosure and Barring Service (DBS) checks;

Information on grievances raised by or involving you;

Information on conduct and/or other disciplinary issues involving you;

Details of your appraisals and performance reviews;

Details of your performance management/improvement plans (if any);

Details of your time and attendance records;

Information regarding your work output;

Information in applications you make for other positions within our organisation;

Information about your use of our IT, communication and other systems, and other monitoring information;

Details of your use of business-related social media, such as LinkedIn;

Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur); and

Details in references about you that we give to others.

**How we collect the information**

We may collect this information from you, your personnel records, the Home Office, pension administrators, your doctors, from medical and occupational health professionals we engage and from our insurance benefit administrators, the DBS, your trade union, other employees, consultants and other professionals we may engage, eg to advise us generally and/or in relation to any grievance, conduct appraisal or performance review procedure. We may also collect information via monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, email and instant messaging systems, Internet facilities, telephones, voicemail, mobile phone records*,* relevant websites and applications.

**Why we collect the information and how we use it**

We will typically collect and use this information for the following purposes (other purposes that may also apply are explained in our data protection policy):

for the performance of a contract with you, or to take steps to enter into a contract;

for compliance with a legal obligation (eg our obligations to you as your employer under employment protection and health safety legislation, and under statutory codes of practice, such as those issued by Acas); and

for the purposes of our legitimate interests or those of a third party (such as a benefits provider), but only if these are not overridden by your interests, rights or freedoms.

Further information on the monitoring we undertake in the workplace and how we do this is available in our Policy and Procedure folder and Employer Handbook, available on the company G drive.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any material changes to information we collect or to the purposes for which we collect and process it.

**How we may share the information**

We may also need to share some of the above categories of personal information with other parties, such as external contractors and our professional advisers and with potential purchasers of some or all of our business or on a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

**Where information may be held**

Information may be held at our offices and third party agencies, service providers, representatives and agents as described above. We have security measures in place to seek to ensure that there is appropriate security for information we hold including those measures detailed in our Data Protection policy.

**How long we keep your information**

We keep your information during and after your employment for no longer than is necessary for the purposes for which the personal information is processed.Further details on this are available in our Record retention policy and Record retention schedule.

**Your rights to correct and access your information and to ask for it to be erased**

Please contact our Data Protection Officer if (in accordance with applicable law) you would like to correct or request access to information that we hold relating to you or if you have any questions about this notice. You also have the right to ask our Data Protection Officer for some but not all of the information we hold and process to be erased (the ‘right to be forgotten’) in certain circumstances. Our Data Protection Officer will provide you with further information about the right to be forgotten, if you ask for it.

**Keeping your personal information secure**

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

**How to complain**

We hope that our Data Protection Officer can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at [ico.org.uk/concerns/](https://ico.org.uk/concerns/) or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Job Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 2**

**AGE UK NORTH CUMBRIA**

**CONFIDENTIALITY POLICY STATEMENT**

The right to privacy in one’s life is the hallmark of a free society and grounded in Legislation. Age UK North Cumbria recognises and endorses this Human right.

Age UK North Cumbria accepts that personal details about an Individual belong to that Individual and the same is true about Organisational data.

We therefore aim to ensure that information which is learned about Individuals and Organisations in the course of our work is treated with absolute confidentiality.

To implement this:

* Age UK North Cumbria will only use information which is learned about Individuals and Organisations for the purpose for which it is given.
* Confidentiality of records will be maintained; access to records will be restricted to those persons who are authorised to see them.
* Information relating to an individual or Organisation will not be given to a third party without specific consent (written or verbal).
* Any unauthorised disclosure of information (verbal, written or implied) will be treated as a very serious matter.

Age UK North Cumbria recognises that Organisations and Individuals (sometimes people who are very vulnerable) place a trust in us, that they are free to confide personal information, and that anything divulged will be treated in the strictest of confidence.

Age UK North Cumbria values this trust highly and will take all reasonable steps to safeguard it.

**Confidentiality of Personal and Organisational information: Regulations for Trustees / Employees / Volunteers and any other Individuals involved in the Organisation.**

1. All personal information concerning Trustees / Employees / Volunteers / Clients and any other Individuals involved in the Organisation is **CONFIDENTIAL.**
2. Information must **NOT** be disclosed to anybody other than in the following circumstances:
   * With the Individual’s or Organisation’s specific consent.
   * Where an Individual is unable to provide meaningful consent to share data, then this must be sought from an Individual’s named legal representative and appropriate evidence is required.
   * To other Employees/ Volunteers/ Individuals involved in the Organisation, to the extent needed to enable them to carry out their work.
   * To others involved in supporting that Individual, to the extent needed to enable them to carry out their work. Examples are NHS workers, Social Workers, other Voluntary Organisations.
   * In exceptional circumstances when the need to protect the health and welfare of the Client or another person overrides the Client’s right to confidentiality. Under these circumstances the Chief Executive only, must authorise this disclosure.
   * When disclosure is required by law.
3. The above confidentiality processes also cover any member of the Client’s wider network.
4. Whenever you are not sure whether information should be disclosed, you must consult the Chief Executive Officer.
5. All information relating to the internal affairs of Age UK North Cumbria is **CONFIDENTIAL**.

I confirm that I must maintain the confidentiality of Individual and Organisational information entrusted to me in the course of my work and I undertake to abide by these regulations.

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Job Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_