Your Data at Age UK
Policy, Procedure and Guidance

When Age UK recruits colleagues, personal data is collected, stored and processed accordingly to manage, administer and support the employment relationship. However Age UK recognises that it is important that this data is handled and protected appropriately, and this document aims to ensure all colleagues are aware of their personal rights in relation to their own data, they understand how their data is handled and stored, how they can control and see their own data held by Age UK and most importantly can be assured of Age UK's commitment to protecting such personal information.

Contents

Policy

1. What is the purpose of this policy?

The purpose of this policy is to set out the means by which Age UK can ensure that all colleagues' personal data is handled appropriately and in line with the requirements of

the General Data Protection Regulation and that colleagues are aware of their rights under this regulation.

2. Who does the policy apply to?

This policy applies to all colleagues of Age UK including fixed term, temporary colleagues, casual workers and agency workers. However the types of data held regarding these colleagues will differ so some sections will apply if appropriate.

3. What is the Age UK policy?

Age UK is committed to ensuring full compliance with all data protection regulations and protecting the privacy of all colleagues, and as such will take all reasonable steps to ensure that colleagues are confident that their data and personal information is handled appropriately and with great care. The procedure therefore helps us to ensure that any colleague handling employee data, understands how this should be handled, stored and processed; we will also continue to raise awareness of the issues surrounding data protection in order that colleagues are careful throughout their work with Age UK, especially where personal and sensitive data is handled as part of that work. Age UK will be transparent to colleagues and those that wish to be considered to come and work for Age UK about their data, why we are asking for certain types of information, how this is stored and processed and for what purpose. Data retention is also constantly under review on the basis that we won't hold any data relating to current or previous colleagues that we are no longer required to retain.

4. Who is responsible for implementing the policy?

Age UK Managers and Heads of Department and those employees with delegated responsibility for team leadership and supervision are responsible for day-to-day implementation of the policy amongst the teams that are directly managed by them. Managers are responsible for reading and understanding this policy and procedure, ensuring they attend any training and complete any online learning regarding data security and for promoting good data governance amongst their teams throughout their work.

Age UK People and Performance (P&P) are responsible for ensuring that people practices including induction, training and awareness reflect the Age UK commitment to excellent data security in relation to colleague data. The P&P team will help to ensure all colleagues have a good general awareness of the requirements of the General Data Protection Regulations and that those colleagues with access to personal data understand their responsibility regarding that data and their handling of it on behalf of the organisation.

Age UK Employees are responsible for their own conduct and behaviour and their duties in respect of their working and day to day activities. Employees are therefore expected to comply with mandatory training activities and ensure they understand the policy in relation to colleague information at Age UK. This may well also extend to other data that they may handle, for example donors, supporters, older people etc. Individual departmental policies and procedures will dictate specific rules and practices in relation to such data that is outside that of employment data.

5. Definitions

For the purpose of this policy, the following definitions are relevant;

- *Personal Data* – in statute, this is defined as data that relates to a living individual who can be identified from such data. For example, even if we removed names from a set of data, individuals may still be identifiable from the data. This could be from their employee number for example or from a postcode that only they hold in rare cases. We have to therefore be careful around identifying colleagues within data. For example, if we shared data that related to a job title that only one person held, it is likely that they can be identifiable from that data.

Personal Data can include a Facebook profile, IP address, Drivers' license number and a home address

- *Special Categories of Personal Data (formally known as sensitive data)* – This is a special form of personal data that requires extra care on the basis that it could be used to unlawfully discriminate against someone. This type of data includes the following:
  1) Racial or ethnic origin
  2) Political opinions
  3) Religious or philosophical beliefs
  4) Trade union membership
  5) Physical or mental health
  6) Sexual life or sexual orientation
  7) Genetic data
  8) Biometric data (such as finger prints)

- *Data Subject* – This relates to the person who is the subject of personal data. In the employment relationship, the data subject will be our colleagues but a data subject can also be a customer, client or donor as well as supplier if they happen to be sole traders.

- *Data controller* – A data controller will ordinarily be an organisation which alone or jointly with others determines the purposes and means of processing of personal data. In this case, Age UK is the data controller.

- *Data processor* – within the legal framework, this is an organisation or individual that processes data on behalf of a data controller. An example of a data processor who works with Age UK would be BUPA, one of our benefit providers as they receive information regarding our employees in order that we can provide a benefit for a health cash plan as part of their contract.

- *Processing* – the law around data protection talks a lot about the "processing" of data, which covers anything with personal data including collecting, recording, organising, structuring, storing, adapting, altering, retrieving or using that data.

Procedure

1. Colleague data held at Age UK

Age UK as an employer holds a significant amount of data in relation to its workforce. This will include data regarding employees, volunteers, contractors and self-employed colleagues.

1.1 The legal framework

The General Data Protection Regulation (GDPR) requires all processing of data to be justified by what is called a "lawful basis for processing". This means that any data that any organisation wishes to process in relation to any individual, where that individual can be identified from such data, must now have a lawful basis for this processing. A lawful basis must fall into one of the following categories:

- It is necessary for the performance of a contract (such as an employment contract)
- It is necessary for fulfilling legal obligations (such as defending a claim or investigating a crime for example)
- It is in the vital interests of either the data subject or some other person (such as holding details about blood group types in hospitals)
- It is in the public interest (this could be in the exercise of official authority)
- It is in the legitimate interests of the organisation (this can include ordinary and honest business practices)

In the event that none of the above apply, an organisation will be required to seek the express consent of the data subject to process their data.

It is important that Age UK identifies a lawful basis for the processing of all data including that which relates to our colleagues. On the basis that colleagues are engaged in a contract of either employment or some other form of contractual engagement, the processing of such information relating to all colleagues will be **necessary for the performance of such contract.**

The following sections provides further detail about the data held, why we hold it, how it is stored and our retention policies in relation to such information.

1.2 Data Held by People & Performance (P&P)

We have carefully reviewed the data that we hold within the P&P team and how this is stored. When candidates express an interest in coming to work for Age UK, they will register on our careers site, which is hosted by TalentLink. This site provides full details relating to how we handle any information provided by candidates, but this information is limited to what is relevant to their application, such as their contact details, unspent criminal convictions under the rehabilitation of offender's act, where they heard about the role and details they provide on the CV and supporting statement. We also ask candidates for some Equality, Diversity and Inclusion information in order that we can ensure that we are reaching out to all sectors of the population, and so that we can reflect on our recruitment processes and decisions ensuring that no discrimination or

even unconscious bias creeps into our practices. This data is not shared with hiring managers, is held securely and does not form part of any decision making during the recruitment process.

Once a candidate has accepted an offer of employment, further details are required, which are necessary for the performance of their contract. Such details include but are not limited to their date of birth, their NI number and bank details, beneficiary details for their life assurance, further Equalities Data for employment monitoring purposes and tax code details.

These are all stored securely on our itrent system and we no longer hold any paper files relating to new starters to the organisation. Only members of the P&P team can access this data with some restrictions according to the level and placement of the colleague.

Given that the itrent system is both a HR and a payroll system, there is no requirement for any data to be moved from the system to share with payroll.

1.3 Data shared with benefit providers and third parties

We are proud to be able to offer a great suite of benefits to our employees and we work with some partner organisations in order to provide these. These organisations include:
BenefitHub– for discount benefits
BUPA – for the healthcare cash plan
Scottish Widows – for pension provision
AVIVA – for life assurance and long-term sickness cover (where this is provided in the contract of employment)
The ELAS Group - for occupational health services
Third party processors who provide operational system support services.

Details relating to these provisions are shared with the appropriate benefit providers in order that these can be made available in accordance with the contract of employment.

BenefitHub require information regarding employee number and date of birth. This information is then required when colleagues register with the service for the first time. Should colleagues wish to register, BenefitHub will then require some further information directly.

BUPA require employee name, employee number, address, date of birth and gender to provide colleagues with access to the benefit.

Our pension provider also require information relating to colleagues' name, address, employment start date, date of birth, nationality, salary, NI number and contribution rates. Regular reports are then provided as and when contributions are applied to the personal pension plan on a monthly basis. This report uses NI number as a unique identifier.

ELAS require name, date of birth, gender, address, contact number, health information and service history. Consent to refer to this service will always be obtained from employees prior to making a referral to ELAS.

As part of the contract of employment we also provide life assurance to our colleagues and in order to do this, we share details with our insurers via our brokers. This information includes name, place of work, NI number, salary, job title, start date, pension scheme membership and level of life assurance cover. We provide this every year upon renewal of the plan. In addition to this, we are also required to provide information relating to any absence from Age UK that is 3 months or more and ongoing. This enables the insurers to fully assess the claims risk and calculate our annual premium, which in turns enables us to provide this benefit to all colleagues.

Age UK also takes a view regarding roles that require a DBS check of varying levels. This check requires Age UK to share information relating to colleagues with our third party provider, GB Group, who carries out the checks on our behalf. When colleagues make their own application for the disclosure, they are required to provide information directly to our provider via an online portal however prior to that, the following information is shared with them in order to set up access to the portal:
Name
Personal email address
Position at Age UK

We will always stipulate within our job advertisements and within the contract of employment when a DBS check is required for a role. Where one is required, Age UK believes that this is necessary and in the legitimate interests of the organisation. The successful candidate will be made aware that their details will be shared with the provider as above.

Please be assured that when we share data with external organisations, this is transferred securely.

1.4 Data held by Age UK Managers

Managers at Age UK will be required to temporarily hold some personal data in order that they can effectively manage their teams. This data will likely include:

- Return to work and absence information
- Notes from 1-1s, informal meetings and performance reviews
- ID documents at the commencement of employment
- Contact details for in the event of a Business Continuity alert or to make contact as needed

This list is not intended to be exhaustive. Any data held locally by managers must be stored securely in a lockable cabinet and these are provided upon request, however we operate a clear desk policy, and we ask colleagues to print only when absolutely necessary, avoiding the printing of personal data wherever possible. Line managers are required to use the itrent and MyLo systems as a means for storing data and

recording check-ins. Within that system they can securely file and further access such information relating to their teams. There should therefore be no requirement for managers to hold data in paper format once a process has concluded. The itrent system is secure and linked to all colleagues' login details. Retail colleagues access their details using a login and password of their choice that meets security requirements. This is therefore the most secure place to retain all information of this nature.

Any data relating to colleagues must never be left unattended or stored in a place that isn't secure / lockable. Please see the Managers Guidance to Colleague Data Security for further details and help.

Managers must be aware of where they are saving files electronically relating to their staff – no one else should have access to these

1.5 Data Held by Colleagues

From time to time, fellow colleagues may require access to information about their team members such as contact details and these should be stored securely only accessible to those colleagues that require such information. Any such information must be securely destroyed at the point at which it is no longer required (e.g. upon the departure of the employee). Where a colleague requires contact details relating to a fellow colleague or volunteer for purposes that aren't work related, we are not able to provide this and instead will suggest that these details are sought directly from that colleague.

1.6 Data Retention

Data retention refers to how long we retain data, and the means by which we destroy it once it is no longer needed. Given data is held within P&P, payroll and the pensions team as well as with our managers, we have different approaches to data retention for these groups, based on their own circumstances and requirements.

The management team – Once a colleague has left the team, there is no longer a requirement for their manager to hold **any** data in relation to them. As long as all documents are held on the itrent system for in the event they may be required or requested, all other paperwork must immediately be destroyed confidentially following that individual's departure. Managers may wish to forward some documents to P&P for uploading to the employees personnel file and/or for confidential waste.

Where any paper copies have been created, these must be destroyed confidentially and safely using either a shredder or a confidential waste organisation as approved by Age UK. Both shops and offices have access to some form of confidential waste as prescribed locally. This should therefore significantly reduce the requirement for managers to hold any paper copies of any such information relating to their teams. In the event that paper copies cannot be destroyed confidentially, these must be forwarded to the P&P team for destroying.

The deletion of data also includes any files that may have been saved to the managers personal F drive.

Managers will cease to have access to their leaver's details within itrent following their departure.

Please refer to the Managers Guidance on Handling Staff Data for more information. Please note that where data is not handled in accordance with this procedure and this could potentially compromise the privacy rights of colleagues, this will be investigated under Age UK's disciplinary policy and procedure.

The People Team– We have data relating to colleagues within both our recruitment system and itrent. Within the recruitment system, we do inform candidates that in the event they are unsuccessful in their application, that their data will be retained on our system for a period of 12 months. This is to allow us to reach out to those candidates again if we have a further opportunity they may wish to be considered for.

We retain data relating to all active employees throughout their employment and this is gathered and stored on their personnel file that is part of the itrent system. Once colleagues have left Age UK, we will retain data for a period of 7 years within the system and this data will be used for in the event we are asked to provide a reference. We do require prospective employers to share evidence of consent from colleagues before any references will be provided. We also retain this data for in the event that it is required for any legal reasons associated with that colleague.

The payroll team – the payroll team have continuing requirements to report to the HMRC even after a colleague has left the organisation and for that reason, they will also retain data for a period of 7 years following an employees' leave date from Age UK. However this data will relate only to payroll matters as payroll do not require access to any other details such as Equality and Diversity information or details relating to training or performance reviews for example.

The pensions team – the pensions team may well be required to provide information relating to pensions well after a colleague has left Age UK and as such, they are required to keep their own records, which are held separately and securely, for a period that can be up to 40 years after normal retirement age. This ensures that we can then be helpful and provide information in the event of any queries relating to personal pension plans after colleagues have left Age UK.

All colleagues will only have access to data they require for their role and will only retain such data for as long as is required.

2. Volunteer Information

Age UK engages with volunteers in a variety of ways and these include:

- Friendship volunteers
- The Silver Line Helpline volunteers
- Retail volunteers in shops

- Events volunteers
- Office volunteers
- Engagement volunteers

We do need to gather some basic information relating to our volunteers and this will vary depending on the way in which they volunteer with us but the information we require will be limited to that which is needed for their role at Age UK. Access to such information will only be provided to those that require it and this data is held by Age UK as we believe that it is within the **legitimate interests of the organisation.**

Information relating to volunteers will be retained by Age UK for a period after their departure from Age UK and we will confirm this period in each case. This varies depending on the role and its circumstances. However, any volunteer, should they wish to no longer work with Age UK, could make a request for us to delete their details from our records.

3. Consultants

From time to time, we have consultants that come to work with Age UK. These colleagues are engaged in a Contract for Services and therefore we collect necessary information for the performance of such a contract. This is therefore the lawful basis upon which this data is processed. We would intend to retain all documents relating to a consultant for a period of 7 years following their departure from Age UK, which is in line with the retention period for employee information.

We do not hold data relating to consultants within our itrent HR system however details are retained in an electronic file held on the Age UK network and only accessible to those that require such information within the P&P team. Additionally our finance colleagues will have access to financial information that is required for the purposes of making payment against invoices.

4. Special categories of data

As well as data considered as “personal” we also process some data relating to our colleagues that is within the special categories of data. These are defined in section 5 but basically incorporate data that requires extra care on the basis that it can be used to unlawfully discriminate against someone. It is for that reason that we limit access to such data. At Age UK, we refer to the following:

1) Medical information – this could be in the form of fit notes and return to work information that is provided to managers both during a period of absence and also at the end of such absence at the return to work interview. We provide clear guidance to managers on the handling of such data. We say that information relating to health and absence should be entered directly into the itrent system where it can only be accessed by the line manager and the colleague concerned as well as those within the P&P team who require access to such information. Such P&P colleagues will not access this unless required.

2) Sensitive information – when individuals apply to work with us and also when join Age UK, they are asked to provide information relating to them personally such as ethnicity, sexual orientation, disability information, caring responsibilities etc. This information helps us to drive our agenda relating to diversity at Age UK. We can then focus activity within certain areas where we need to raise the profile of certain groups at Age UK. We are continually monitoring our procedures to ensure they apply fairly to all and to ensure that Age UK continues to be an inclusive employer. This information helps us to do this and identify areas for improvement. We understand that this information is highly sensitive and personal to colleagues so we don't ask for paper copies to be submitted but instead allow colleagues to directly enter this onto their own self service account confidentially. Managers cannot access this in self-service – only a small number of senior colleagues within the P&P team can access this.

3) Trade union membership – We do not ask our recognised trade union about membership numbers or names. Colleagues may well chose to inform Age UK of their trade union membership but this information isn't otherwise shared with Age UK.

5. Further data privacy rights

Under the data protection legislation, we all as "data subjects" have a number of rights in relation to the data that organisations hold about us. It is important that employers and employees all have an understanding of these rights in order that we can ensure colleagues understand how they can make certain requests and that our management team understand how they can acquiesce. These rights are summarised below with some further guidance:

Rectification

Employees are entitled to ask their employer to deal with any issues with the accuracy of the data that we hold about them. Therefore, if any colleague feels that their data held by Age UK is incorrect in anyway, please contact your P&P representative in order to make arrangements for it to be changed. In some cases, this may require further investigation in order to understand how the error has come about and to help ensure we avoid a similar situation moving forward.

The right to be forgotten

Colleagues, along with any other data subject, do have the "right to be forgotten" under the legal framework and this essentially means that we can make contact with organisations who hold data about us and can make a request for them to confidentially destroy such data. We may find from time to time that colleagues, upon leaving Age UK, may submit a request to be forgotten and for Age UK to delete all data they hold about that individual. Where there is an alternative requirement for holding such data, it will not be possible for Age UK to comply with this. For example, we hold employee details once colleagues have left for the following reasons:

- Pension plan details
- HMRC notifications and reporting
- Defending potential claims (during periods in which claims can still be bought against the charity)
- To provide references to colleagues that have left the organisation and are actively securing employment elsewhere

Be aware that where a colleague submits a request to be forgotten, where we are able to comply with this request, this will mean that we will no longer be able to provide a reference for that colleague in relation to their time at Age UK. Any requests for references will receive a response that indicates that we hold no record relating to the employment to which they refer.

Any requests under this right must be submitted in writing to the People & Performance department, where they can be considered further in line with any other requirements to continue to retain such data. We will endeavour to respond to such requests with full reasons in the event that we aren't able to delete the information held.

Restriction of processing
Often where colleagues aren't able to ask an organisation to erase their data, they may well be able to ask them to restrict the processing of such data. This means that we may be able to consider how this data is processed in line with a request which will also need to take into account the ongoing requirements to hold or process that data. For example, a colleague may well wish to make a request that their personnel file is no longer held by Age UK, but that minimal details are retained for the purposes of providing a reference. These requests would be considered on a case by case basis and once a request has been received in writing, we can then consider and respond accordingly with full reasons.

6. Colleague access to data

All "data subjects" have a legal right to access data that any organisation holds about them. This right also extends to colleagues at Age UK and therefore all people have a right to access the data that Age UK holds about them. Requests of this nature are to be submitted to your People Team representative at which point the request will be further considered. The Subject Access Request Form can be used in order that colleagues can be clear on their request and what they require.

In addition to the form, ex-colleagues will also be asked to verify their identity in order that the information and data can be shared safely with them. This condition has been applied in order that we handle colleague data in a safe and secure manner.

There is no longer any fee payable to Age UK for such a request to be supported and processed. Age UK will respond to such a request within 28 days of receipt of this request in writing using the above form.

There may be some circumstances under which the organisation may need to give further consideration to such a request, and this may be the case whereby the request

is potentially unfounded, excessive or is repetitive. In this event, full reasons will be provided in the event that a request is declined or a fee is requested due to the circumstances.

7. Monitoring activity at Age UK

As a large employer covering a number of establishments, including our retail shops, we do handle some information relating to our colleagues that is as a result of monitoring activity. Monitoring activity can include the following:

- CCTV footage (in retail)
- Mystery shopper information (in retail)
- Some monitoring activity around email traffic – please see the User Security Policy and the Information Security Policy for more detail relating to this
- Charity vehicle tracking system (for Stock Collectors in retail)
- Locker and bag checks (in retail)

All details relating to any monitoring activity within retail is outlined in further detail in the Monitoring (Retail) Policy and Procedure.

We use privacy impact assessments to ensure that newly proposed monitoring activity doesn't compromise the privacy rights of those colleagues that will be impacted. Privacy impact assessments are useful tools that allow us to consider alternative methods of monitoring to that which is proposed and also to consider whether the monitoring activity is proportionate and justified. Any such privacy impact assessment will be subject to the approval of the senior management team. Please see the Monitoring (Retail) Policy and Procedure for more details.

8. Requests for information from external organisations

From time to time, Age UK works with outside organisations to provide services and help to provide a good suite of benefits for colleagues. Any such sharing of information will always be limited to what is required only and will be moved in a secure manner with benefit providers using secure portals. Information is shared with external organisations for the following:

- For death in service and income protection benefits as appropriate
- Some monitoring activities within the retail division (see the Retail Monitoring Policy and Procedure for further information)
- BenefitHub (for the discounts that employees are entitled to as part of their contract)
- BUPA (to provide the healthcare scheme to employees in accordance with their contract of employment)
- Wellbeing providers (this is as and when colleagues register for a service or class such as a massage or to have an appointment with the nutritionist)
- Scottish Widows (our pension provider)

9. Data incidents or concerns

Please be assured that Age UK has endeavoured to engage a number of measures with the aim of preventing any such risks to our colleagues' data. Such work and associated measures are constantly reviewed - as the online environment changes and develops. Unfortunately, from time to time organisations have found themselves in breach of data protection legislation, often not through fault of their own however circumstances may arise that can involve unlawful hacking events or penetration of systems, or sometimes unfortunate acts that can have consequences for our colleagues if this relates to their data. Age UK takes a very strict approach to such events and would always seek to take all appropriate and reasonable measures in such an event.

Potential data breaches may include the theft of a workplace laptop, unauthorised access to recruitment records and a system hacking attack, theft of data, unforeseen circumstances such as fire or theft, human error, to name a few. A personal data breach is formally defined as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Where Age UK becomes aware of concerns regarding data security that concerns our colleagues and their information and data, the following steps will be taken:

1) An investigation will be undertaken to establish the circumstances of the potential breach and what action can be taken to minimise risk to colleagues, if any are identified
2) Any mitigating actions will be considered and then taken immediately in order to reduce the risk to colleagues
3) A full report will be submitted to Age UK's Director of Information Protection and Compliance, Head of Legal, HR Director and any other relevant senior colleague depending on the circumstances at which point a paper and advice note will be produced for Age UK Directors to make a decision on next steps
4) At this stage, a formal decision will be made regarding next steps and this will include a decision regarding a formal notification to the Information Commissioners Office (ICO), which is the governing body for all data protection and privacy regulations. This notification will be made where it is felt that the incident is likely to, or could, result in risk to colleagues
5) Age UK will then work together with the ICO to continue investigations and support the ICO investigation into such event – the ICO may well provide further guidance to Age UK as well as make formal decisions regarding the incident. Age UK will always co-operate with the ICO in such event.

This notification to the ICO must take place where feasible within 72 hours of us becoming aware of the incident or event.

In addition to this, where the event may well pose a significant risk to those affected, Age UK will also seek to notify those colleagues on an individual basis of the event and provide any further details and support, as reasonably practical. The decision regarding this type of direct communication will be guided by our ability to implement measures to protect the data and whether we have been able to significantly reduce the risk to those impacted. We may also make a decision not to do this where such communication would require significant disproportionate effort. These factors will all be balanced against our aim to be transparent and honest with colleagues that may be impacted.

Where colleagues have concerns or questions following such a communication, Age UK will take steps to provide further assurance and detail as required and necessary.

10. Our Colleagues employed by The Silver Line Helpline

This policy and procedure also applies to colleagues within the Silver Line Helpline. Arrangements are being made to move employee data to itrent and hard copy personnel files to the Age UK Ashburton site. In the meantime, payroll information is currently contained within Sage software and hard copy personnel files are contained securely within the Blackpool office, with access limited to The Silver Line management. More recent contracts of employments, amendments to contracts, and employee relations case notes are stored electronically by the P&P department in a secure manner.

11. Further information

There are a number of accompanying documents that provide more detail and guidance relating to specific areas. These include:

- Your Data at Age UK – Guidance for Candidates Applying to Work at Age UK
- Your Data at Age UK – Guidance for Managers Handling Colleague's Personal Data
- Age UK Information Security Policies – available on the loop
- Age UK Group Data Protection Policy

For further advice relating to your data at Age UK, please speak to your P&P representative. For more general advice relating to data protection at Age UK, please contact the Director of Information Protection and Compliance.

Document version control

This policy and procedure will be reviewed regularly or at a minimum on a bi-yearly basis, or at the point of any significant change in legislation (whichever occurs first).

Version Number	Date	Action Taken	Next review due
Version 1	April 2018	Policy written, consulted on and published	April 2020

Version 2	April 2022	Policy Reviewed and created new section for TSL colleagues	April 2024