Data Protection Policy

Introduction

Data protection is about ensuring people can trust organisations to use their data fairly and responsibly. The UK data protection regime is set out in the Data Protection Act 2018 along with the GDPR (General Data Protection Regulations) (which also forms part of UK law). The Information Commissioners Office (ICO) regulates data protection in the UK.

The following is not a definitive statement on the Act, but seeks to interpret relevant points where they affect Age UK Lewisham & Southwark.

The Act covers both written and computerised information and the individual's right to see such records.

It is important to note that the Act covers all records relating to clients, staff and volunteers

All Age UK Lewisham & Southwark staff and volunteers are required to follow this Data Protection Policy and Procedures at all times. Failure to do so may lead to disciplinary procedures.

The Chief Executive has overall responsibility for data protection within Age UK Lewisham & Southwark but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

Definitions

Processing of information – how information is held and managed.
Data Subject – used to denote an individual about whom data is held.

Data Controller – used to denote the entity with overall responsibility for data collection and management. Age UK Lewisham & Southwark is the Data Controller for the purposes of the Act.

Data Processor – an individual handling or processing data

Personal data – any information about a particular living individual which can identify who they are. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public.
Special categories of personal data – Some of the personal data processed can be more sensitive in nature and therefore requires a higher level of protection. The GDPR refers to the processing of these data as 'special categories of personal data'. This means personal data about an individual's:

- race
- ethnic origin
- political opinions,
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- health data
- sex life or sexual orientation

Data Protection Principles

Everyone responsible for using personal data must ensure that the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Individual's Rights

Under the Data Protection Act 2018 individuals have the right to find out what information Age UK Lewisham & Southwark hold about them. These include the right to:

- Be informed about how data is being used
- Access personal data
- Have incorrect data updated
- Have data erased
- Stop or restrict the processing of their data
- Data portability (allowing the individual to get and reuse their data for different services)
- Object to how their data is processed in certain circumstances.

Procedures

Lawful Basis

Data Protection regulations state that in order to collect, process and store data Consent must be obtained at the point of collection from the data subject UNLESS the need to do so falls within one of the lawful grounds that does not require consent.

Those grounds are where it is necessary for the:

1) Performance of a Contract
2) Compliance with Legal Obligations
3) Protection of the Vital Interests of the data subject (or another)
4) Performance of a task earned out in Public Interest or in exercise of Official Authority
5) Purposes of Legitimate Interests pursued by the Data Controller

Age UK Lewisham and Southwark will be using Legitimate Interest as the most appropriate basis for collecting, process and storing the personal data of our service users. The rationale for this is that in order to effectively deliver services individuals would have a reasonable expectation that a certain amount of data would need to be provided to enable an assessment of need to be carried out and the appropriate package of support be provided to the service user.

In using this ground a Legitimate Interest Assessment has been completed outlining the necessity for using legitimate interest rather than Consent and the steps taken to demonstrate how using legitimate interest provides a clear benefit to the individual.

Consent will still be sought where identifiable personal data will be used for certain activities relating to marketing, publicity, social media, photographs, etc.

Ensuring the Security of Personal Information

1. It is an offence to disclose personal information ‘knowingly and recklessly’ to third parties.

2. Personal information should only be communicated within Age UK Lewisham & Southwark’s staff and volunteer team on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

Ethnic Monitoring

Age UK Lewisham & Southwark wishes to be an inclusive organisation. In order for Age UK Lewisham & Southwark to monitor how well our staff, volunteers and service users reflect the diversity of the local community we request that they complete an Equality and Diversity Monitoring form. The completion of the form is voluntary, although strongly encouraged. Responses are securely stored and held on a passworded database for statistical and monitoring purposes. Where the details are required for reporting to a funder the information will be anonymised.

Use of Files, Books and 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.

Disposal of Scrap Paper, Printing or Photocopying Overruns

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.

Computers

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

Computer monitors in the reception area, or other public areas, should be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection. If working in a public area, eg reception, you should lock your computer when leaving it unattended.

Firewalls and virus protection to be employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Documents should only be stored on the server or cloud-based systems and not on individual computers.

Where computers or other mobile devices are taken for use off the premises the device must be password protected.

If accessing emails, databases or other work related data from a personal device such as mobile phone, tablet, laptop etc, you should ensure that adequate firewall and virus protection is installed at all times. You should also ensure that your device is password protected and that confidentiality is maintained so that others cannot have access to Age UK Lewisham & Southwark data.

Cloud Computing

When commissioning cloud based systems, Age UK Lewisham & Southwark will satisfy themselves as to the compliance of data protection principles and robustness of the cloud based providers.

Age UK Lewisham & Southwark currently uses two cloud based data management systems to hold and manage information about its service users and donors/supporters.

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 Lewisham & Southwark is satisfied with the security levels in place to protect its data.

Sharepoint O365

SharePoint, hosted by Microsoft, holds data about Age UK Lewisham & Southwark's activities, this includes; volunteer data, employee data, client data and financial data. 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.

Xero

Xero, hosted by Amazon Web Services, holds data about Age UK Lewisham and Southwark's employee's salaries and income and expenditure. Access is password protected and restricted to named users.

My HR Toolkit

My HR Toolkit, hosted by Agilio Group, holds data about Age UK Lewisham & Southwark's employees and volunteer. Access is password protected and restricted to named users. My HR Toolkit is headquartered in Sheffield, England.

Direct Marketing

Direct Marketing is a communication that seeks to elicit a measurable fundraising response (such as a donation, a visit to a website, sign up to Gift Aid, etc.). The communication may be in any of a variety of formats including mail, telemarketing and email. The responses should be recorded to inform the next communication. Age UK Lewisham & Southwark will not share or sell its database(s) with outside organisations.

Age UK Lewisham & Southwark holds information on our staff, volunteers, clients and other supporters, to whom we will from time to time send copies of our newsletters, magazine and details of other activities that may be of interest to them. Specific consent to contact will be sought from our, clients and other supporters, including which formats they prefer (eg mail, email, phone etc) before making any communications.

We recognise that clients, staff, volunteers and supporters for whom we hold records have the right to unsubscribe from our mailing lists. This wish will be recorded on their records and will be excluded from future contacts.

Age UK Lewisham & Southwark will not undertake direct telephone marketing activities under any circumstances.

Privacy Statements

A Privacy Statement will also be published on our website explaining:

- Who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out

.

All service users will receive a summary Privacy Notice when their consents are obtained. This Notice will explain what information we hold and why.

Staff and Volunteers will receive a detailed Privacy Notice upon appointment explaining the various pieces of information held and why.

Personnel Records

The Regulations apply equally to volunteer and staff records.
For staff and volunteers who are regularly involved with vulnerable adults, it will be necessary for Age UK Lewisham & Southwark to apply to the Disclosure & Barring Service (DBS) 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 the Leadership Team. If there is a positive disclosure the Chief Executive will discuss this with the individual and the Leadership Team member. (Please refer to our Policy on the Disclosure & Barring Service.) Staff and volunteers who are subject to DBS checks, must disclose any convictions, cautions, reprimands and final warnings which are issued to them after the DBS check has taken place. If there is a subsequent disclosure the Chief Executive will discuss this, anonymously, with our insurers to assess the risk of continued appointment.

Confidentiality

Further guidance regarding confidentiality issues can be found in our Confidentiality Policy.

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All electronic data, e.g. documents and programmes related to work for Age UK Lewisham & Southwark should not be stored on any external hard disk or on a personal computer. If documents need to be worked on at a non-networked device they should be saved onto a USB drive which should be password protected or encrypted.

Workstations in areas accessible to the public, e.g. reception or trading office, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it and consideration should be given to what may be seen on screens. All screens should be locked when not in use.

When sending emails or other electronic communications to outside organisations, e.g. social worker or hospital staff, care should be taken to ensure that any identifying data is removed and that codes (e.g. initials or identifying code number, such as social services number, etc.) are to be used. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork kept away from the office (e.g. clients care plan kept at home by a worker) should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (e.g. on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement. Enablers needing to take paperwork away from a client's home (e.g. unable to make a required phone call during the visit) must ensure that it is returned to the client's home on the next visit.

If you are carrying documents relating to a number of clients when on a series of home visits, you should keep the documents for other clients locked out of sight in the boot of the car (not on the front seat) and not take them into the client's home. When carrying paper files or documents they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain Age UK Lewisham & Southwark's contact details. Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a client's home with the correct number of documents and that you haven't inadvertently left something behind.

Retention of Records

Retention of records

This table sets out minimum periods we will keep records (whether paper or electronic)

Type of record	Minimum retention period	Other information
Personnel files including documentation of grievance and disciplinary processes	7 years from the end of the individual's employment	Commitment to provide employment references and in case of litigation

Type of record	Minimum retention period	Other information
Details of trustees	7 years after they cease to be trustees	
All information relating to redundancies involving less than 20 staff	7 years from the date of the redundancy	
All information relating to redundancies involving more than 20 staff	7 years from the date of the redundancy	
All records relating to maternity, paternity, adoption and parental leave pay	7 years from the end of the tax year they relate to	
Governance and constitutional documentation	12 years from any change in the documentation or from the point in time that the document is superseded	
Client legal files (incl. client complaints)	7 years after the closure of the case.	To be in a position to respond to any further legal action
Client enquiry forms	18 months (unless a full client file open in which case it is kept as part of that file)	
All primary financial documentation including payroll information, invoices, signed accounts	7 years	

Type of record	Minimum retention period	Other information
Contracts	7 years from the end of the contract	
Returns to financial authorities (HMRC and pension providers)	7 years	
Policies	7 years from the amendment of the policy or the point in time when it is superseded	
Application forms and selection process documentation	1 year	To be able to respond to any challenge to the recruitment/selection and appointment process
All documentation relating to accidents	7 years from the date of the last reported incident	
All Health & Safety compliance records	Until superseded by later records	
Reports from external bodies specifically regarding any aspect of AUKLS activities	7 years (longer in specific instances)	This does not include reports of general interest that have not been compiled specifically about Navigate
Health records (general)	During employment only	
Health records relating to the termination of employment	7 years	To be able to respond to any legal action

Type of record	Minimum retention period	Other information
Governance documents including those outlining constitutional matters as well as minutes and resolutions	Permanently or 7 years after they have been superseded	
Insurance documents	7 years	To be able to respond to any legal action

Note - The above minimums will be extended in the event of any specific requirements instituted by the approved authorities or where AUKLS enters in to any contractual arrangement where a longer retention period for documentation is specified.

Off-site archived records should clearly display the destruction date.

Computerised records e.g. Charitylog, to be anonymised seven 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.) Minimal data may be kept for the purposes of identifying legacies in the future.

Please see Record Keeping Policy for information on destruction process.

What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you should report this to your line manager and Director of Operations who will review our systems to prevent a reoccurrence. The Director of Operation should note the 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 the Director of Operations should be informed without delay.

In the event that the breach involves clients receiving a service commissioned by Lewisham Council or Southwark Council information (eg day services or enabling), the relevant council should be informed by the Chief Executive by email.

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.

Subject Access Requests (SARs)

Data Subjects can ask, in writing to the Chief Executive, to see all personal data held on them, including e-mails and computer or paper files. The Data Controller (Age UK Lewisham & Southwark) must comply with such requests within 30 days of receipt of the written request.

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

Further Information

Further information is available at www.informationcommissioner.gov.uk

Details of the Information Commissioner

The Information Commissioner's office is at:

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Switchboard*:* 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 0303 123 1113
Notification Line: 0303 123 1113