Data Protection Policy

V3.0 February 2026

This Policy explains how ELCAP use (or, to use the legal terminology, 'Process') the Personal Data of actual or prospective service users and staff, as well as donors, business contacts, suppliers and other third parties.

It applies to all Personal Data we use, regardless of the media on which it is stored.

Data protection is the responsibility of everyone within the organisation. This Policy sets out what we expect from all our staff when handling it to enable us to comply with applicable law.

Your compliance is mandatory. You must read, understand and comply with this Policy when using Personal Data on our behalf and attend training on its requirements, in particular where you have a specific responsibility, such as providing service users with legally required information, documenting consent, or reporting a Personal Data Breach. Related ELCAP policies provide additional guidance to help ensure you act in accordance with this policy and the relevant law.

Any breach of this Data Protection Policy may result in disciplinary action.

Definitions and terminology used in this policy are explained in the relevant section. For ease, they are also listed in alphabetical order within the Appendix, with a further brief explanation.

Important reminder: Data protection law requires ELCAP to investigate and document any personal data breach. We have a procedure to deal with these. In some situations, these must be reported to the Information Commissioner and, in limited situations, we are required to notify the individuals impacted.

If you know or suspect that a Personal Data Breach has occurred, refer to our internal **Data Breach Reporting Procedure**.

Scope of Policy, and when to seek advice on data protection compliance

Protecting confidentiality, and the integrity and security of Personal Data, is a critical responsibility which we take seriously.

All staff at ELCAP are responsible for ensuring the organisation's compliance with data protection law. We all need to adhere to appropriate practices, processes, controls and training to ensure that compliance.

Please contact ELCAP's Senior Management Team or Business Manager with any questions about the operation of this Policy or if you have any concerns that it is not being or has not been followed, particularly in the following circumstances:

(a) if you suspect there has been a Personal Data Breach;

(b) if you need any assistance dealing with any rights invoked by individual or complaints about how we use personal data;

(c) whenever you are engaging in a significant new, or change in, use of personal data which is likely to require a Data Protection Impact Assessment (DPIA) as described in the 'definitions' section of this Policy;

(d) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making, as described later in this policy;

(e) if you need guidance on applicable law when carrying out any direct marketing activities (which is defined by law to include fundraising activities); or

(f) if you need guidance in relation to sharing Personal Data outside ELCAP

Personal data protection principles

We adhere to general principles relating to Processing of Personal Data set out by law, which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

(b) collected only for specified, explicit and legitimate purposes (purpose limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

(d) accurate and where necessary kept up to date (accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

(g) not transferred to another country without appropriate safeguards in place (transfer limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

Further guidance on each of these general principles is given below.

Lawfulness, fairness and transparency

Personal data must be Processed lawfully, fairly and in a transparent manner.

These restrictions are not intended to prevent Processing, but rather to ensure that organisations Process Personal Data fairly, and without adversely affecting individuals.

In practice, ELCAP may only collect, process and share Personal Data fairly and for specified lawful purposes, which are when:

(a) the Processing is necessary for the performance of a contract with the individual;

(b) the Processing is necessary to meet our legal compliance obligations;

(c) the Processing is necessary to protect the individual's (or another individuals) vital interests, for example in an emergency situation;

(d) the Processing is necessary to pursue legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of other individuals.; or

(e) the individual has given their Consent.

Transparency

Data protection laws require ELCAP to provide detailed, specific information to individuals about how we use personal data.

We do this through an appropriate Privacy Policy. Our website provides a Privacy policy for prospective and actual service users, and other individuals outside ELCAP such as donors, available at https://www.elcap.org/privacy-policy/

Separately we have a privacy policy for actual or prospective staff (including volunteers and interns and individual self-employed contractors who work for ELCAP).

If you are collecting Personal Data from individuals on behalf of ELCAP then you must provide or direct individuals to the relevant privacy policy, so they have to this information.

It is a legal requirement for the information to be "concise, transparent, intelligible, easily accessible, and in clear and plain language" so that individuals can easily understand it.

In situations where you are concerned that a particular individual might not find our policy satisfies those requirements, for example where a specific individual experiences difficulties reading, or has a health condition which impacts on their abilities, please contact the Business Manager for guidance.

ELCAP also have responsibilities when Personal Data is collected indirectly (for example, from a third party or publicly available source). We are expected to check, in a situation where the Personal Data was collected by the third party, that it was done in accordance with the law (in particular, with a lawful basis covering our proposed use or 'Processing' of that Personal Data.) We may be required to provide the individual or individuals concerned with all the legally required

information in our policy as soon as possible after collecting or receiving their personal data, if that has not already been done by the third party.

Purpose limitation

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

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

If you want to use Personal Data for a new or different purpose from that for which it was obtained, contact our Business Manager for guidance on how to do this in compliance with the law and this Policy.

Data minimisation

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

You may only Process Personal Data when performing your work duties requires it. You cannot Process Personal Data for any reason unrelated to those duties.

Only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is relevant and adequate for the intended purposes.

When Personal Data is no longer needed for specified purposes, it is deleted (or anonymised) in accordance with ELCAP's retention guidelines.

Accuracy

Personal Data must be accurate and, where necessary, kept up to date.

You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You are expected to check the accuracy of any Personal Data at the point of collection and at regular appropriate intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data. It must be corrected or deleted without delay when inaccurate.

Storage limitation

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

Our retention policies and procedures ensure Personal Data is deleted in accordance with the law. You are expected to take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our retention practices and policies. This includes requiring third parties to delete that data where applicable.

When individuals request information about the period for which personal data is stored, please seek guidance from our Business Manager to ensure they are given the relevant information from our retention policies.

Security integrity and confidentiality

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

We have implemented and maintain safeguards appropriate to our size, scope and activities, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and risks we have identified (including use of encryption and Pseudonymisation where applicable).

We operate reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. With support from our security advisors and service providers, we evaluate and test the effectiveness of those safeguards to ensure security of our Personal Data Processing.

All staff share responsibilities for helping to safeguard and protect the Personal Data we hold. You must follow all procedures and use the technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

You may only transfer Personal Data to authorised third-party service providers who meet our security requirements and have put adequate security measures in place. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must help to maintain data security by protecting the confidentiality, integrity and availability of the Personal Data:

(a) Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

(b) Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of all related policies which ensure security, in particular our Computers, Internet and Email Policy, our Confidentiality Policy, our Cyber Security Policy, and our Homeworking & Hybrid Working Policy You must not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain.

It is essential, should you change the device that you use for work purposes, that you link with the Administration Team so that any new device can be registered with Access Care Planning so that you can access that platform for work purposes.

International transfer limitations

Data protection law restricts transfers of personal data to countries outside the UK to ensure that the level protection afforded to individuals is not undermined. A transfer occurs when we send, transmit, view or access that data in or to a different country.

Please seek guidance from our Business Manager, in conjunction with IT Provider before any international transfer.

Individual rights and requests

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

(a) receive certain information about our Processing activities, which are available in the relevant ELCAP privacy policy;

(b) request access to their Personal Data that we hold (including receiving a copy of their Personal Data);

(c) withdraw Consent to Processing at any time;

(d) prevent our use of their Personal Data for direct marketing or fundraising purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) object to Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of any agreement under which Personal Data is transferred outside of the UK;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breaches which are likely to result in high risk to their rights and freedoms;

(l) make a complaint to us and subsequently to the supervisory authority;

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

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

You must immediately forward any request described above or complaint received about how ELCAP Process Personal Data to our Business Manager.

12. Record Keeping

Data Protection laws require ELCAP to keep full accurate records of our data Processing activities.

You must support ELCAP in creating and maintaining accurate records reflecting our Processing, for example records of individual's Consents, in accordance with our internal procedures and policies.

Consent

ELCAP rely on different lawful bases when we use personal data. There are some situations in which we rely upon an Individual's consent to Processing of their Personal Data.

Here is a summary of the legal requirements when we do:

- We must take care and make sure that individuals have been made aware of ELCAP's privacy policy before giving consent in order to make sure that a legally valid Consent has been given.
- You will need to evidence Consent has been collected in accordance with the law and keep records in accordance with our internal policies, so that we can demonstrate compliance.
- Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to collect consent from an individual.
- If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.
- An individual must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured.
- Consent may need to be refreshed if we intend to use Personal Data for a different and incompatible purpose which was not disclosed when the individual first consented.

Training and audit

We are required to ensure all staff receive adequate training to enable them to comply with data protection laws.

You must undergo all mandatory Personal Data or data privacy-related training and ensure your team completes mandatory training in accordance with any instructions issued.

We must also regularly audit and test our systems and processes to assess compliance with data protection laws. You are expected to regularly review compliance with all the processes and systems under your control to ensure they operate in compliance with this Data Protection Policy, confirming and checking that adequate governance controls and resources are in place and operating to ensure proper use and protection of Personal Data.

Direct marketing, including fundraising

ELCAP, like all organisations, are subject to rules and privacy laws when engaging in direct marketing to prospective and actual service users and/or donors (which includes, for example, when sending fundraising emails or making telephone calls).

An individual's consent is generally required for electronic direct messaging (for example, by email, text or automated calls) if one of the message's purposes includes marketing or promoting ELCAP (or another organisation) or fundraising activities.

The limited exception is known as "soft opt-in" which allows us to send such messages without consent if

(a) the sole purpose is furthering our charitable purposes;

(b) contact details were obtained when individuals expressed interest in or supported those purposes; and

(c) recipients were given an opportunity to 'opt out' of electronic messaging when we first collected contact details and that opportunity is given in every subsequent marketing message.

You must only send electronic messages for direct marketing as permitted by law, explained in this guidance. You must discuss with your line manager if you are unsure about how to comply with this guidance in practice.

It is explained in our privacy policies that individuals have the right to object to direct marketing. Any objection must always be promptly actioned.

If an actual or prospective service user or donor "Friend of ELCAP" 'opts out' at any time, their details should be 'suppressed' as soon as possible. ('Suppression' involves retaining just enough information to ensure that their messaging preferences are respected in the future). Those individuals' details (contact information) are kept within a spreadsheet held securely in SharePoint. It is also contained in the personal profile of the individual on Access Care Planning and Access People Planner.

Consents for use of information or photographs reflecting good news or achievements are documented in a separate media permission form. Copies of these are stored within SharePoint and Access Care Planning platforms to inform and secure compliance

"Friends of ELCAP" personal details are held on a spreadsheet for Ebulletins and newsletter information sharing, including AGM dates and organisational updates.

Sharing Personal Data

You may only share Personal Data we hold with other staff where they have a work-related need to know the information and sharing complies with our policies.

Generally, we are not allowed to share Personal Data outside ELCAP with third parties (individuals and/or organisations) unless certain safeguards and contractual arrangements are in place.

However, guidance from the ICO explains that Data sharing is lawful in an urgent situation or in an emergency which includes:

- preventing serious physical harm to a person;
- preventing loss of human life;
- protection of public health;
- safeguarding vulnerable adults or children;
- responding to an emergency; or
- an immediate need to protect national security.

Aside from those limited situations, you may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data is in line with ELCAP's Privacy Policy which explains the extent to which we share Personal Data

(c) and, if required, the individual's Consent has been obtained.

Appendix: Definitions

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

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of Artificial Intelligence (AI) where they involve the processing of Personal Data.

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

Controller: the person or organisation that determines when, why and how to process Personal Data. It is the organisation responsible for establishing practices and policies in line with data protection laws. ELCAP are the Controller of all Personal Data relating to our Personnel and Personal Data used in our organisation.

Criminal Offence Data: as defined by law to include personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

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

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of compliance with 'Privacy by Design' legal obligations. They should be done for all major system or change programmes involving the Processing of Personal Data.

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

UK GDPR: a version of the General Data Protection Regulation (*(EU) 2016/679*) retained in UK law following our departure from the European Union (Brexit).

Personal Data: any information identifying a Data Subject, or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.

Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data, which are described in this list of definitions. It does not include anonymous data (i.e. data where the identity of an individual has been permanently removed).

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Appendix 1 lists the types of personal data that ELCAP collect and input on Access relating to individuals we work with and Appendix 2 lists types relating to our staff.

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

Privacy by Design: an expression taken from law, which means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Policies: ELCAP policies setting out information that must be available or provided to individuals when we collect personal data.

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

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers (e.g. pseudonyms, unique numeric identifiers) so that the named person to whom the data relates cannot be identified without the use of additional information. This is a measure to help protect confidentiality and security of personal data. Such data it remains within scope of 'personal data' as defined by law.

Related Policies: ELCAP policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available internally.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

ELCAP uses sensitive data about support that individuals we work with may require, made accessible to staff who are supporting them. This information includes information about their family, representatives, Guardians and Social Work depending on the framework tailored to the individual. We also use sensitive data about our staff members, for example where that information is necessary to ensure accurate support to a colleague. We protect such sensitive data with the same care as when we use 'special categories' of personal data, as defined by law.

Appendix 1

PERSONAL DATA COLLECTED FOR ACCESS - INDIVIDUALS

General

- Type of service
- Title, First Name, Middle Initial, Surname, Preferred Name
- Address
- Postcode
- Date of Birth
- Start date of service
- Service Priority
- Locality of Work
- Service of Work

Contact

- Home Number / Mobile
- Personal email address

Access

- Details of key safe number and location for secure access to property

Equality

- Gender
- Marital Status
- Ethnic Origin
- Religion
- (All options have the opportunity to state "prefer not to say")

Other

- Mosaic Number / Contract number from Local Authority / Commissioner
- Details of documents checked
- Record of any restrictions

Photo Permission

- Newsletter / Profile Only / Recruitment / Social Media / Website

Emergency contacts

Medical Details

Service Funder Details

Contracted Hours

Training / Qualifications required for your support

Tasks

- Guardianship
- Tenancy agreement
- DNACPR
- Intensive Housing Management Details
- Signed contract
- Support Plan details
- Risk Assessments
- Review of Support
- Funeral arrangements
- Finance details

Equipment

List of equipment that we support you with for maintenance and renewal

Rota Planning

- Shift allocation, matched with staff allocated to your service provision and necessary training required to best meet your needs

Support Planning

- Details of your all support needs and guidance for staff to ensure they follow your preferences, needs and wishes during support time
- Team Meetings and reviews relating to your support to ensure that we meet your requirements.

Appendix 2

PERSONAL DATA COLLECTED FOR ACCESS - STAFF

General

- Title, First Name, Middle Initial, Surname, Preferred Name
- Address
- Postcode
- Date of Birth
- Start date
- First Date of Shift (automated from Rota Planning)
- Last date of shift (Automated from rota planning)
- Role Type
- Working Time Directive
- Locality of Work
- Service of Work

Communication

- Home Number / Mobile
- Personal email address & ELCAP email address

Equality

- Gender
- Sexuality
- Marital Status
- Nationality
- Ethnic Origin
- Religion
- (All options have the opportunity to state "prefer not to say")

Eligibility

- Right to Work Check documents
- Details of documents checked
- Record of any restrictions

Payroll

- NI Number

- Payroll type
- Payroll Number
- Rate Sheet

Holiday

- Entitlement which then auto calculate data inputted for holidays

Travel

- Mode of transport
- Details of credentials for Business Insurance and Licence Type

Bank

- Bank Details
- (Permissions are set that data processors and finance team have access to this information)

Background

Identified background in care experience

Disabilities

- Disclosure of any disabilities and details of any reasonable adjustments

Personal Data

- Emergency Contacts
- Critical Information
- Availability
- Medical Details (if disclosed)
- Equipment issued by ELCAP
- Training & Qualifications
- (These are tracked with renewal dates and also used to match training with individual needs configured within the system)
- Tasks
- Onboarding tasks and ongoing supervision and support tasks

Other information

- SSSC details including registration number, conditions and reregistration date
- PVG details including membership number, issue date and revalidation date
- Media Consent (Profile only, website, social media, recruitment and newsletter options to select)

Photograph

Obtained for RTW authentication check and personnel profile including ID badge

Reports

The reports are created by ELCAP pulling identified data fields from both platforms to create data reporting elements for individuals, staff and other data fields.