Policy

Policy number	**3.37**
Subject	**Data Protection**
Directorate responsible	**Quality**
Date last reviewed/by whom	December 2023 – Anthony Heppell Assistant Director of Quality and Safeguarding
Date to be reviewed	December 2025

Linkage Community Trust's Data Protection Policy has been produced to ensure compliance with the General Data Protection Regulation (GDPR) and associated legislation, such as the Data Protection Act 2018. This policy incorporates guidance from the Information Commissioner's Office (ICO) and other relevant organisations.
The Policy provides a framework for compliance and will be supported by a series of additional policies and guidance documents focusing on specific areas of data compliance within the Trust. The guidance documents will be used to provide advice and keep staff up to date with good practice.

Objectives

The Policy's objectives are:

- To ensure staff are aware of the statutory duties the GDPR and other relevant data protection legislation places on the Trust.
- To ensure staff are aware of their legal obligations and responsibilities under the GDPR and other relevant data protection legislation.
- To provide clarity to staff on key aspects of data protection legislation.
- To ensure staff are aware compliance with this policy and associated legislation is a requirement and any member of staff who fails to comply may be subject to disciplinary action.

Help with this Policy
Guidance and clarification about the interpretation or any other aspect of this policy is available from the Data Protection Officer who can be contacted at dataprotection@linkage.org.uk

Who is covered by this Policy?
This policy applies to all staff at Linkage. This includes temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of the Trust.

What Data is covered by the Policy?
This policy is concerned with personal data (including Special Category data) as defined by the GDPR. Personal data is any information relating to a living individual who can be directly or indirectly identified, by reference to an identifier, such as a name, an identification number, location data, or an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Examples of categories of personal data include:

- Name
- Date of birth
- Address
- National insurance number
- Passport number
- Payroll number
- Student ID
- Comments made about an individual in email
- IP address

Special Category (formerly known as sensitive personal) data is a subset of personal data and means personal data consisting of information relating to.Racial or ethnic origin

- Political opinions
- Religious or philosophical beliefs
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Genetic data (used for identifying an individual)
- Biometric data (used for identifying an individual)
- Data concerning an individual's health
- An individual's sex life or sexual orientation

Any processing of criminal offence data should be handled similarly to Special Category data, by determining the legal basis of processing in accordance with Article 6 of the Data Protection Act, with the condition of also ensuring compliance with Article 10. Collecting, or further processing criminal offence data, should be approved by the Data Protection Officer they can be contacted at dataprotection@linkage.org.uk

The Data Protection Legislation

Data protection legislation (GDPR and the Data Protection Act 2018) provides a framework for organisations (controllers) which ensures personal data is handled properly, as well as providing legal rights to individuals (data subjects). The legislation works in two ways: firstly, it states anyone who processes personal data must comply with the data protection principles, as defined by the relevant data protection legislation; secondly, it provides individuals with important rights, including the right to find out what personal data is held, about them, in both digital and paper records.

The Data Protection Principles

Data protection legislation requires the Trust (as a controller), its staff and others who process or use any personal data to comply with the data protection principles. The principles are listed below:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Rights of Individuals

The GDPR, provides various rights to individuals, these are listed below

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights relating to automated decision-making including profiling

If any member of the Trust receives a request relating to any of the above rights it must be sent immediately to the Data Protection Officer who will process it. It should be sent to dataprotection@linkage.org.uk

The most exercised individual right is that of the right of access. The right of access allows an individual to know what information the Trust holds and processes about them. This is known as a subject access request, which also provides for individuals to be given a copy of the information, as well as supplementary

information, such as where and with whom the information may have been shared. The right of access, like many individual rights, is not an absolute right and disclosure of the requested information is subject to exemptions.

Unless the information requested is provided as part of the normal course of business, the individual who is the subject of the data (the data subject) should be directed to the Data Protection Officer they can be contacted at dataprotection@linkage.org.uk for advice on how to make a Subject Access Request (SAR). The Trust must respond to these requests within one month of their receipt.

Registration and Notification

As a data controller, the Trust is required to register with the Information Commissioner's Office (ICO) and submit an annual notification listing the purposes under which it processes personal information. The Trust must also notify the ICO within 28 days should any entry become inaccurate or incomplete. The ICO publishes a register of controllers on its website which is available to the public for inspection. The Trust's notification can be found on the ICO's website by entering its registration number: Z1029093

It is an offence for the Trust to process personal data that falls outside of the purposes declared in its notification, unless these are exempt. Staff who work with personal data should be familiar with the notification and inform the Data Protection Officer if they intend to implement changes that may require the notification to be amended.

The Information Commissioner's Office

The ICO is the UK's independent authority (Supervisory Authority) established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO enforces and oversees the relevant data protection legislation as well as the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations. The ICO has the power to take regulatory actions to enforce compliance with the data protection legislation which include enforcement notices, audit, monetary penalties (up to a maximum of 4% of the controller's gross annual turnover or €20,000,000 whichever is higher).

The ICO also receives and responds to complaints from individuals and organisations who feel they are being denied access to personal data they are entitled to or feel their information has not been handled according to the data protection principles or legislation. Communication with the ICO is conducted by the Data Protection Officer. If you are contacted by them, please contact dataprotection@linkage.org.uk

Further information about the ICO can be found on its website at http://www.ico.org.uk

Responsibilities

Staff who process personal data as part of their duties must ensure they are complying with the Data Protection Principles described in section 3.1, and more generally in compliance with relevant data protection legislation. "Processing" data is a collective term for any action taken relating to personal data and includes obtaining, recording, storing, using, sharing, disclosing, transferring, or destroying data.

Obtaining Personal Data

Only personal data necessary for a specific Trust-related business reason should be obtained, and it should be collected in a secure manner.

A privacy notice (also known as a fair processing notice) must be actively communicated to an individual at the point their personal data is collected, and subsequently if requested by individuals. Ideally the privacy notice should be provided in the same medium, in which the data was collected. A privacy notice must as a minimum include the following:

- The name and contact details of the Controller
- Contact details of the Data Protection Officer(s)

- The purposes of the processing
- The legal basis of this processing
- Details regarding any processing based on legitimate interest
- Categories of personal data being processed
- The recipients or categories of recipients of the personal data
- Details regarding any transfers of personal data to a third country, or international organisations
- Retention periods for the personal data
- Information regarding individual rights
- The right to withdraw consent (if this is the basis of the processing)
- How to make a complaint, and how to do so
- Details of any statutory or contractual processing
- The existence of any automated decision making, including profiling
- Details of any examples where the controller is likely to process the personal data for a different purpose than it was originally collected

In some cases, individuals will have a choice as to whether to provide their personal data, or the use that can be made of it. In these cases, clear consent must be obtained. All consent mechanisms must be compliant with the threshold stipulated by the GDPR. 'Optout' consent is no longer valid.

New Processing

When new projects and initiatives are being developed within the Trust that could have implications on individuals' privacy, the Data Protection Officer should be consulted. Where the project has a technical element or relies on software IT should also be contacted to identify and assess any privacy concerns. A Data Protection Impact Assessment (DPIA) must be completed; when a new purpose or project will include the processing of personal data, when there is any high risk (including large scale) processing, and when new technology is introduced. The DPIA screening questions at Annex 3 should be answered. Answering yes to any of those questions will mean a complete DPIA is required, to undertake this please contact dataprotection@linkage.org.uk

Staff must comply with the concept of Data Protection by Design and Default. This is a mandatory concept enforced by the GDPR, from the beginning and throughout the lifecycle of personal data.
Data Protection by Design and Default requires controllers to implement appropriate technical and organisational measures:

- Which are designed to implement the data protection principles.
- Ensuring that, by default, only the minimal amount of personal data is processed for each of the processing purposes. (This is when privacy enhancing techniques, such as anonymization and pseudonymisation, should be considered)

Recording Personal Data

Staff must ensure mechanisms are in place for keeping personal data accurate and up-to date and for the purpose for which it is held.

Personal data should be retained in accordance with any retention period specified in the relevant privacy notice, and in accordance with the Records Retention Schedule.
Staff should be aware that any material they produce which refers to an individual (or individuals) may be accessed by the individual, regardless of the informality of the information, how or where it is held, including data held in email accounts. This includes any opinion of or about the individual. Staff should be aware of this when documents/records are created, including emails.

Emails

Linkage provides their staff with email accounts. These email accounts and the information contained within are a corporate asset and as such the data is processed and controlled by the Trust. The email accounts of staff may be accessed for several reasons including but not limited to, processing a right to access request, mitigating a data breach and to assist with any misconduct investigation(s). Staff should not be using private email addresses to undertake Linkage work, any email addresses that have Trust data in may be accessed by the Trust.

Processes

Staff whose work involves processing personal data, whether in electronic or paper form, must take personal responsibility for its secure storage.
Access to personal data, in electronic or paper form, should be restricted to staff who need to access the information in the course of their duties.
Personal data in paper form must be kept in a lockable filing cabinet, cupboard, drawer or behind a locked door.
Documents containing personal data should only be printed when there is a business need to do so.
Staff who intend to store personal data on a portable storage device, such as a laptop, tablet, memory stick, hard drive, disk or mobile phone, must seek the authorisation of their line manager. The personal data on the portable storage device must be encrypted and the device must be kept in a lockable filing cabinet, cupboard or drawer.
Staff must not keep special category data on portable storage devices unless they have received authorisation from both their line manager and the Data
Protection Officer.
Personal data should never be routinely stored at staff members' homes, whether in paper or electronic form. In instances where off-site processing is necessary, staff must obtain authorisation from their line manager. If the processing includes special category (sensitive) data, the authorisation of both their line manager and the Head of
Department is required. It is strongly recommended that the advice of the Data Protection Officer is sought

If personal data are processed off-site electronically, this must be done so using Trust approved equipment and/or systems (including remote access mechanisms)
When processing personal data, a Clear Desk must be adhered to by all staff and managed by line managers, see **3.26 Clear Desk Policy**.

Using Personal Data

Personal data should only be processed for the specific purpose contained in the relevant privacy notice which was provided when the data was collected.

If staff wish to use the personal data in a new and unforeseen way the Data Protection Officer should be contacted to review the relevant Privacy Notice. If the change is not reasonably expected by the data subjects, staff must actively communicate the revised privacy notice to them. In certain cases, clear consent from the data subjects must be obtained before the personal data is used in the new way. Data Protection by Design and Default must be considered throughout the lifecycle of personal data.

Staff should be aware of the possible risk of unauthorised persons viewing personal data displayed on computer screens or in paper documents, particularly in open plan offices.
Preventative measures such as facing computer screens away from high traffic or public areas and taking care not to leave documents containing personal data in view, should be taken. The use of privacy filters on computer screens should also be considered: a review of privacy filters should be considered by line managers.

Marketing

All marketing activities, including communications which involve processing personal data must be managed in accordance with both the GDPR and the Privacy and Electronic

Communication Regulation (PECR). Unsolicited marketing activities involving messages sent by

telephone, fax, email or text must conform to GDPR and PECR. If you process personal data for these purposes, you must consult with the Data Protection Officer before any activity takes place.

Sharing and Disclosing Personal Data

When personal data is shared between departments for valid business reasons the data must be relevant and the minimum necessary to achieve the objective. Any sharing of documents containing personal data, including special category data, could be shared using SharePoint.

Files and folders can be shared using links to documents rather than sent as an attachment.

If a file must be shared as an attachment (e.g. due file type), it must be either password and/or encryption protected, using tools such as Zip compression software. When using a
password to protect the data, it must be conveyed to the recipient in a separate message. Best practice is to relay the password by telephone to the intended recipient.

Following sharing, departments must assess whether any new use of data will be compatible with the purpose for which it was originally collected. If not, the data subjects may need to be made aware of the intention to use their data in this way and in some instances, consent may be required. In addition, the DPIA screening questions will need to be considered.

Retention and Disposal

Departments must also consider the retention and disposal of shared information. Where the data is required for a single purpose, the duplicate information should be destroyed after use. Where a permanent record is required, the department must establish a process to ensure the data continues to be held in line with the Data Protection Principles and the Retention Schedule. Further guidance on sharing data internally is available from the Data Protection Officer.

Third Party Processing

In some instances, the Trust is required, for mandatory or statutory reasons, to share information with certain third parties outside of the Trust. Personal data may also be shared with other third parties; if there is a clear and lawful purpose for doing so, if the data sharing is a proportionate means of achieving that purpose, and if the data sharing is transparent to the data subjects. Further guidance on sharing data with third parties is available from the Data Protection Officer. In most cases, where the sharing of data is regular, then an information sharing agreement between the parties is required. Template information sharing agreements can be obtained from the Data Protection Officer.

The Trust as the controller continues to remain liable for ensuring personal data is processed in compliance with the Data Protection Principles, when the processing is undertaken by an external company or organisation (known as a data processor). Although the processor is now also liable for any inappropriate processing activities. If a department decides to outsource a data processing function, it must ensure a data processing agreement is in place before any activity is undertaken by the processor, on the controller's behalf. There is a
necessity to provide assurance the data processor will meet their legal obligations as stipulated by relevant data protection legislation, which are known as 'sufficient guarantees'.

The Data Protection Officer must be made aware of any intention to engage a data processor so that up-to-date guidance can be provided to ensure all documents, including contracts, are compliant with relevant data protection legislation. When finalised, a signed copy of the data processing agreement should be sent to the Data Protection Officer.

Relevant data protection legislation allows the disclosure of personal data to authorised bodies, such as the

Police and other organisations that have a crime prevention or law
enforcement function. Staff who receive a request to disclose personal data for reasons relating to national

security, crime prevention or taxation should contact the Data Protection Officer for advice.

In response to most other requests, staff must not disclose personal data, or particularly special category (sensitive) data, without the consent of the data subject. (However, in some cases consent may not be appropriate, and the Data Protection Officer should be contacted for assistance). If consent is received, staff must ensure that the data is given to the correct enquirer: for this reason, disclosure should be made in writing and not by telephone. If a request for the disclosure of personal data is received, and consent has not been given by the data subject, the request should be sent to the Data Protection Officer to process appropriately.

If personal details are requested by a data subject or third party that is not provided as part of normal business, the individual requesting the data should be directed to the Data Protection Officer for advice on how to make a Subject Access Request (SAR). The Trust must respond to SARs within one month of their receipt.

Transferring Personal Data within the Trust

Any transfer of personal data must be done securely.

Email carries a high level of risk and should not be routinely used for sending personal information. Sending personal data via external email should be avoided unless it is:

- encrypted, with the password provided to the recipient by separate means (such as via telephone).
- by other encryption techniques.
- or using a link to shared folders or with suitable access control.

While internal email is more secure, it is still advisable to consider encrypting attachments which contain data belonging to many data subjects, or sensitive personal data, to mitigate the risks associated with emails being sent or forwarded to unintended recipients.
Emails containing personal data should have an appropriate subject heading and explain clearly to the recipient why they are being sent the information, and what they are expected to do with it.
Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important emails are correctly addressed and care is taken when using the 'Reply All', forwarding functions, or when copying others into emails.

Personal email accounts must not be used to send or receive personal data for work purposes.
When sending personal data externally, by paper form, a Royal Mail tracking service or courier service must be used. If personal data is sent via Royal Mail, it is recommended the 'Special Delivery' service is used, particularly if Special Category data is being transferred.

When sending personal data internally in paper form, it should be sealed in an envelope marked confidential' and ideally hand-delivered to the recipient.

Destroying Personal Data

Departments should adhere to the Trust's Record Retention Schedule for all data (including personal data) they hold and ensure it is destroyed when n longer required. The retention periods specified within privacy notices should be reflected in the Records Retention Schedule.

On destruction, personal data in paper form must be shredded and/or sealed in the confidential waste bags. Personal data in electronic form should be deleted. Portable devices that hold personal data can be destroyed by IT Services if office shredders do not include this capability.

Reporting a Data Breach

It is important the Trust responds to data breaches quickly and effectively. A breach may arise from; a theft, a deliberate attack on systems, unauthorised use of personal data, accidental loss, by disclosure (including emails, containing personal data being sent to the wrong recipient), or equipment failure. Data

breaches should be reported to Data Protection Officer and/or IT Services as soon as possible so mitigation techniques can be implemented quickly to limit any potential repercussions.
The Data Protection Officer has produced guidance, and this should be followed for all data breaches. The document should be sent to dataprotection@linkage.org.uk

Responsibilities

Data Protection Officer

It is the responsibility of the Data Protection Officer to process all personal data breaches. Where these involve an IT aspect, they should still be reported to the Data Protection Officer in the first instance, this should be done by using the incident reporting form in Appendix 3.37.01.

The Data Protection Officer will control or mitigate the breach and where necessary report the incident to the Information Commissioner's Office. The Data Protection Officer will also take the decision whether the affected data subjects should be notified. The Data Protection Officer will work closely with individuals and departments to ensure future breaches are preventable.

IT Services

IT services should be contacted when the technical issue does not involve personal data. Examples include malware detections on user devices, DDos attacks, data breaches that only include corporate sensitive data but no personal data, etc.

Data Protection Impact Assessments

Data Protection Impact Assessment screening questions

1. Will the project involve the processing of new (or additional) types of information about individuals
2. Will the project result in the processing of personal data that would have previously required a DPIA?
3. Will the project compel individuals to provide information about themselves, before they can make use of the service provided
4. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information including third party processors
5. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used.
6. Does the project involve processing sensitive ("Special Category") personal data?
7. Does the project involve the personal data of vulnerable people?
8. Does the project involve processing personal data on a large scale?
9. Does the project involve systematic monitoring?
10. Does the project involve the use or application of innovative technological or organisational solutions?
11. Does the project involve automated decision-making that may have a significant effect on an individual?
12. Does the project involve evaluating or scoring individuals (including profiling and predicting)?
13. Does the project involve datasets that have been matched or combined?
14. Is the data transferred internationally?

Answering yes to any of these questions means a Data Protection Impact Assessment is required

Data Breaches

Data breaches can occur through human error or malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. This
guidance note process for responding to any reported data security breach, to ensure the Trust acts responsibly and protects its information assets as far as possible.

Aim

The aim of this guide is to describe the Trust's wide response to any reported data breach incidents and ensure that they are appropriately logged and managed. This will be achieved by adopting a standardised consistent approach to all reported incidents to ensure that:

- Incidents are reported in a timely manner and can be properly investigated,
- Incidents are handled by appropriately authorised and skilled personnel,
- Appropriate levels of Trust management are involved in response management,
- Incidents are recorded and documented,
- The impact of the incidents are understood and action is taken to prevent further damage,
- Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny,
- External bodies or data subjects are informed as required,
- The incidents are dealt with in a timely manner and normal operations restored,
- The incidents are reviewed to identify improvements in policies and procedures.

Definition

A data breach is "any loss of, or unauthorised access to Trust data".
Examples of data breaches may include

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential Trust data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit

For the purposes of this guidance data breaches include both confirmed and suspected incidents that involve personal data. Personal data is defined as any data that can identify an individual.

Scope

This guidance applies to all Trust information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the Trust. It is to be read in conjunction with the Trust's Information Security Policy.

Responsibilities

Information users

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with
investigations as required, particularly if urgent action must be taken to prevent further damage.

Heads of /Department

Heads of Departments are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

Contact Details

The Data Protection Officer who will be investigating breaches and suspected breaches, can be contacted via dataprotection@linkage.org.uk

Data Classification

Data breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the Trust is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

Public Data
Information intended for public use, or information which can be made public without any negative impact for the Trust

Internal Data
Information regarding the day-to-day business operations of the Trust.
Primarily for staff and student use, though some information may be useful to third parties who work with the Trust

Restricted Data
Information of a more sensitive nature for the business and academic operations of the Trust, representing the basic intellectual capital and knowledge.
Access should be limited to only those people that need to know as part of their role within the Trust

Highly Restricted Data
Information that, if released, will cause significant damage to the Trust's business activities or reputation or would lead to breach of the Data Protection Act. Access to this information should be highly restricted

Data Security Breach Reporting
Confirmed or suspected data security breaches should be reported promptly to the Data Protection

Officer email: dataprotection@linkage.org.uk the report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved.
Where possible the incident report form should be completed as part of the reporting process.
See **Appendix 3.37.01.**
Once a data breach has been reported an initial assessment will be made to establish the severity of the breach.

All data security breaches will be centrally logged by the Data Protection Officer to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

Data Breach Management Plan
The management response to any reported data security breach will involve the following four elements.

- Containment and Recovery
- Assessment of Risks
- Consideration of Further Notification
- Evaluation and Response

Authority
Staff, people we support, students, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

Review
The Data Protection Officer will monitor the effectiveness of this guidance and carry out regular reviews of all reported breaches.