No. 20a Data Protection Policy

Version Number	Amendments Made	Date
1	Use of CCTV added (section 12) New Template Use of Multi Factor Authentication Links with other policies section 20	6/10/24
2	Full Review and Updated by Hope and May (DPO)	24/4/26
3	Updates made on the roles and responsibilities and definitions	03/11/26

Approved by	Brendan Dunphy
Date of Issue	November 26
Review due (date)	November 28

Contents

1. Introduction 2
2. Who This Policy Is For 2
3. Aims 2
4. Legislation and Guidance 3
5. Definitions 3
6. The Data Controller 5
7. Roles and responsibilities 5

7.1 Governing Board 5

7.2 Senior Information Risk Owner (SIRO)/Data Protection Officer (DPO)/Information Asset Owners (IAO) 5

7.3 All Staff 6

8. Data Protection Principles 6
9. Collecting Personal Data 7

9.1. Lawfulness, Fairness, and Transparency 7

9.2. Limitation, Minimisation, and Accuracy 8

10. Sharing Personal Data 8

10.1. Data sharing - working with other organisations 9
11. Subject Access Requests and Other Rights of Individuals 10
11.1. Subject Access Requests 10
11.2. Children and Subject Access Requests 11
11.3. Responding to Subject Access Requests 11
11.4. Other Data Protection Rights of the Individual 12
12. CCTV 13
13. Photographs and Videos 13
14. Data Protection by Design and Default 14
15. Data Security and Storage of Records 14
16. Disposal of Records 15
17. Personal Data Breaches 15
18. Training 16
19. Monitoring Arrangements 16
20. International Data Transfer 16
21. Changes to this policy 16
22. Complaints Process 16
23. Links with Other Policies 17
Appendix 1 Personal data breach procedure 17

1. Introduction

The Lowdown's Data Protection Policy is set out below and ensures compliance with data protection best practice and that data is processed lawfully, fairly and in a transparent manner.

2. Who This Policy Is For

This policy is to set out clearly for staff, students, volunteers, trustees, schools, partner agencies, and any others with whom The Lowdown and its subsidiaries may interact, how confidential data will be managed by The Lowdown.

3. Aims

The Lowdown aims to ensure that all personal data collected about staff, students, volunteers, young people, service users, parents/carers, trustees, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

4. Legislation and Guidance

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

5. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity. Personal data does not include data which is entirely anonymous, or the identity has been permanently removed making it impossible to link back to the data subject
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics

	• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes. • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, disclosing, or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Data Protection Officer	DPOs assist an organisation to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO). The DPO of The Lowdown is an outsourced consultancy, **Hope and May, contactable at sofiya@hope-may.com.**
Information Commissioner's Office	The UK's independent authority set up to uphold information rights in the public interest.

6. The Data Controller

The Lowdown processes personal data relating to parents, young people, service users, staff, students, volunteers, trustees, visitors, and others, and therefore is a data controller.

The Lowdown is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

7. Roles and responsibilities

This policy applies to all staff, volunteers and students working for The Lowdown, and to external organisations or individuals working on our behalf. Those who do not comply with this policy may face disciplinary action.

7.1 Governing Board

The governing board has overall responsibility for ensuring that The Lowdown complies with all relevant data protection obligations. The Lowdown's Caldicott Guardian has specific responsibility for ensuring compliance to the Caldicott Principles. The holder of this role is specified on The Lowdown's meet our team page on the website and also in Breathe HR.

7.2 Senior Information Risk Owner (SIRO)/Data Protection Officer (DPO)/Information Asset Owners (IAO)

The Senior Information Risk Owner (SIRO, CEO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

The Lowdown's Senior Information Risk Owner is the CEO of The Lowdown.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on the organisation's data protection issues.

The Data Protection Officer is the first point of contact for individuals whose data the Organisation processes and is the first point of contact for the Information Commissioner's Office (ICO: https://ico.org.uk) in this case. The DPO is responsible for reporting all other data breaches.

The Information Asset Owner (IAO) are The Lowdown's management team and are the nominated owner for one or more identified information assets of the organisation.

IAO's support the organisation's SIRO in their overall information risk management function as defined in the organisation's policy.

All data protection roles within The Lowdown are kept up to date on the following register:

https://digital.nhs.uk/services/organisation-data-service/view-or-update-registers

Or you can contact us by telephone on 01604 634 385.

7.3 All Staff

Staff, volunteers, and student placements are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy.
- Informing the Organisation of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside The Lowdown.
    - If there has been a data breach or a subject access request or request for deletion.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

8. Data Protection Principles

The UK GDPR is based on data protection principles that The Lowdown must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.
- The data subject must be permitted to exercise their rights in relation to their personal data.

- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
- The data subject should be given the option to opt out of sharing their data for research and planning processes.

This policy sets out how the organisation aims to comply with these principles.

9. Collecting Personal Data

9.1. Lawfulness, Fairness, and Transparency

Personal data will only be processed where one of the six lawful bases (legal reasons) under data protection law applies:

- The data needs to be processed so that the organisation can fulfil a contract with the individual, or the individual has asked the organisation to take specific steps before entering a contract.
- The data needs to be processed so that the organisation can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed so that The Lowdown, as a public authority, can perform a task in the public interest, and carry out its official functions.
- The data needs to be processed for the legitimate interests of the organisation or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

When services are offered to young people under 13, parental consent will be obtained.

When personal data is initially collected directly from individuals, they will be provided with the relevant information required by data protection law.

9.2. Limitation, Minimisation, and Accuracy

Personal data will only be collected for specified, explicit, and legitimate purposes. These purposes will be clearly explained to individuals at the point their data is first collected.

If there is an intention to use personal data for purposes beyond those originally stated, individuals will be informed in advance, and consent will be sought where required

Staff must only process personal data where it is necessary to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised in line with the record retention policy.

10. Sharing Personal Data

Personal data will not normally be shared with third parties; however, it may be shared where:

- There is an issue with a young person/service user or parent/carer that puts the safety of themselves, others or staff at risk.
- Where liaison with other agencies is necessary, consent will be sought where required before doing so.
- Where suppliers or contractors require access to personal data to deliver services to staff and service users (for example, IT companies), appropriate measures will be taken to ensure this is managed securely and in line with data protection requirements.
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

Personal data will also be shared with law enforcement and government bodies where there is a legal obligation to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, if personal data is sufficiently anonymised, or consent has been provided.

- Personal data may also be shared with emergency services and local authorities where necessary to support their response to an emergency affecting any service users or staff.

10.1. Data sharing - working with other organisations

As with any other organisation, The Lowdown may collaborate with:

- data processors
- joint controllers
- separate controllers

All third parties engaged who have or may have access to personal data relating to data subjects will either comply with this policy, or it will be ensured that their data protection policies align with it.

A data processor is a company, organisation or individual who is not an employee or volunteer, that processes data on behalf of the data controller (The Lowdown in this policy). Before deciding to use a particular service, the organisation would check the terms and conditions and decide whether it is compliant before deciding to use that service. With freelancers, external researchers and IT companies, the organisation stipulates a Processing Agreement, or a contract including data protection provisions, as outlined by Article 28.3 of the UK GDPR.

Article 26 of the UK GDPR defines *joint controllers* as 'two or more data controllers which jointly determine the purpose and means of processing. When The Lowdown collaborates with a data controller, the parties must agree to a Joint Controller Agreement which could include the following:

- who it applies to.
- general data protection principles, including the basic principle of confidentiality.
- the purposes for which information will be shared.
- the lawful basis on which sharing will take place.
- how each partner will discharge their transparency obligations, and whether all parties will use the same form of words to ensure consistency.
- procedures for sharing information, and in particular for obtaining and recording consent from the data subject (if this is the lawful basis).

- procedures to ensure that all parties have the same understanding of how to comply with the data protection principles regarding data quality and retention.

- access and security procedures.

- procedures for ensuring that the handling of data subjects' rights is consistent and fully compliant.

- procedures for raising concerns or resolving difficulties.

- how the agreement will be managed and kept under review.

The purpose for which information will be shared, the lawful basis on which the sharing will take place and general information about each data controller will need to be included in the privacy notice for those data subjects affected by the data sharing and collaboration between the organisation and the joint controller.

11. Subject Access Requests and Other Rights of Individuals

11.1. Subject Access Requests

Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the organisation holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with?
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period.
- The source of the data.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests can be made in any form, including in writing or verbally, and do not even need to use the wording 'subject access request'. If a data subject makes contact asking for all their data for example, this would still count as a valid SAR request. Once a SAR request is received, the DPO must be notified of the details linked to the request. They should include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

If staff receive a subject access request, they must immediately forward it to the DPO.

11.2. Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of young people aged 13 and over may not be granted without the express permission of the young person. Subject access requests from parents or carers of young people aged 12 and under may be granted without the express permission of the individual. However, this is not a rule and a young person's ability to understand their rights will always be judged on a case-by-case basis.

11.3. Responding to Subject Access Requests

When responding to requests, the organisation:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- In cases where a request is complex or numerous, the organisation may inform the individual that it will respond within three months of receipt. This will be communicated within one month of the request, along with an explanation as to why the extension is necessary.

Information will not be disclosed where it:

- Might cause serious harm to the physical or mental health of the individual or that of another.
- Would reveal that the individual is at risk of abuse, where the disclosure of that information would not be in the individual's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the individual.

If a request is manifestly unfounded or excessive, it may be refused, or a reasonable fee may be charged, considering the administrative costs involved.

There are various factors to consider when deliberating whether a request is manifestly unfounded or excessive. An example that may fall under this wording is if a request is repetitive or asks for further copies of the same information. The decision to refuse a request based on it being manifestly unfounded or excessive should ultimately be left to the DPO.

Where a request is refused, the individual will be informed of the reasons for the refusal and advised of their right to submit a complaint to the Information Commissioner's Office (ICO).

11.4. Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (as outlined above), and the right to receive information at the point of data collection about how personal data is used and processed (see section 9), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask to be informed about how their personal data is being used.
- Ask to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified based on public interest.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).

Additional rights of data subjects include:

- The right to claim damages should they suffer any loss because of a breach.
- The right to complain and the right to request that the ICO carry out an assessment.

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. CCTV

CCTV is used across various locations around The Lowdown's site to ensure the safety of clients, staff, and visitors. The organisation adheres to the Information Commissioner's Office (ICO) code of practice for the use of CCTV.

Individual consent is not required for the use of CCTV; however, clear notification is provided where recording takes place. Security cameras are visibly positioned and supported by prominent signage indicating that CCTV is in operation.

Any enquiries about the CCTV system should be directed to The Lowdown's Office Manager.

13. Photographs and Videos

As part of The Lowdown's activities, photographs may be taken and images of individuals may be recorded.

Written consent will be obtained from parents or carers before photographs or videos are taken of their child for communication, marketing, or promotional purposes. Clear information will be provided to both the parent or carer and the service user (where under 18) regarding how the photograph and/or video will be used.

Uses may include:

- Within the organisation on notice boards and in publications, brochures, newsletters, etc.
- Outside of the organisation by external agencies such as newspapers.
- Online on The Lowdown website or social media pages.

Consent may be refused or withdrawn at any time. Where consent is withdrawn, the photograph or video will be deleted and will not be used or shared further.

When photographs and videos are used in this way, they will not be accompanied by any additional personal information that could enable the child to be identified.

Written consent will be obtained from staff volunteers and students to use photos and videos of them and this consent can again be withdrawn at any time. Their name and role in the organisation will be used in this case if consent is granted.

14. Data Protection by Design and Default

Measures will be implemented to demonstrate that data protection has been integrated into all data processing activities, including:

- Ensuring that the DPO has the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 8).
- Completing privacy impact assessments where the organisation's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; a record of attendance will be kept.
- Carry out an impact assessment review when personal data is involved at the start of a project or if there are any process changes to identify and minimise the risk of managing personal data.
- Regular reviews and audits will be conducted to assess privacy measures and ensure ongoing compliance.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, the name and contact details of The Lowdown and the DPO, along with all required information about how personal data is used and processed, will be made available through privacy notices.
    - An internal record will be maintained for all personal data held, detailing the type of data, the data subjects, how and why the data is used, any third-party recipients, how and why it is stored, applicable retention periods, and the measures in place to ensure its security.

15. Data Security and Storage of Records

Personal data will be protected and kept secure against unauthorised or unlawful access, alteration, processing, or disclosure, as well as against accidental or unlawful loss, destruction, or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.

- Papers containing confidential personal data must not be left on desks, tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords that are at least 12 characters long containing letters and numbers are used to access organisation computers, laptops and other electronic devices. Staff and young people (where appropriate) are reminded to change their passwords at regular intervals. Multi factor Authentication via an email or mobile phone-based authenticator are also in place for all software applications.
- All software and devices should be kept regularly updated for security purposes.
- Encryption software is used to protect all portable devices and removable media, such as USB devices.
- Staff and trustees who store personal information on their personal devices are expected to follow the same security procedures as for organisation-owned equipment.
- Secure wi-fi is to be always used and unsecure public wi-fi should be avoided. Hotspot should be used where personal data needs to be accessed and secure wi-fi is unavailable.
- Staff must use the BCC function when sending group emails where recipients should not know each other's identities or contact details.
- Where personal data needs to be shared with a third party, due diligence will be carried out and reasonable steps taken to ensure that the data is stored securely and adequately protected (see section 10).

16. Disposal of Records

Personal data that is no longer required will be disposed of securely. Data that has become inaccurate or out of date will also be securely disposed of where it is not necessary or possible to rectify or update it.

For example, paper-based records will be put in confidential waste and disposed or securely and electronic files will be overwritten or deleted. Where a third party is engaged to dispose of records on behalf of the organisation, sufficient assurances will be obtained to ensure that the third party complies with data protection law.

17. Personal Data Breaches

The Lowdown will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the procedure set out in Appendix 1 will be followed.

Where appropriate, data breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person.
- The theft of a laptop containing non-encrypted personal data about service users.

18. Training

All staff, volunteers and student placements are provided with data protection training as part of their induction process. This is eLearning training provided by NHS healthcare Training - https://portal.elfh.org.uk/.

Data protection will also form part of continuing professional development at least annually or where changes to legislation, guidance or the organisation's processes make it necessary.

Essential and Advanced training sessions on data protection are also provided by Hope and May.

19. Monitoring Arrangements

The SIRO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if any changes are made to the Data Protection Act 2018 that affect The Lowdown's practice. Otherwise, this policy will be reviewed by the governing body annually.

20. International Data Transfer

Where personal data is stored outside of the UK and the EU, safeguards to protect personal data may include, but are not limited to, the UK Addendum used in conjunction with the EU Standard Contractual Clauses (SCCs), or UK International Data Transfer Agreement (IDTAs). Such safeguards will be subject to Transfer Risk Assessments (TRAs).

21. Changes to this policy

This Policy is updated regularly by the Data Protection Lead when required. It is reviewed annually by the SIRO and the board of trustees.

22. Complaints Process

What Is a Data Protection Complaint?

A data protection complaint is defined as any expression of dissatisfaction regarding the way in which the organisation processes a data subject's personal information. Some examples include:

- Our methods of processing their personal data.
- Failure to respond to a data subject rights request.
- Alleged misuse, loss or inaccuracy of personal data.
- Concerns about transparency, retention or sharing.

Complaints may be received via email, phone, webform, post, or verbally. All staff must treat any such expression of concern as a potential data protection complaint.

Process for dealing with a complaint:

- All staff must recognise and promptly report any expression of dissatisfaction relating to personal data and must forward complaints to their line manager and/or the DPO without undue delay.
- The DPO will then investigate the complaint and respond to the complainant within 30 days. In the investigation, appropriate systems and records will be assessed. The DPO will include the relevant staff members in the investigation.
- Once the investigation is complete, the DPO will send the final response to the complainant with the results of their investigation, and the steps taken to resolve the complaint.
- If the complainant is still unsatisfied with how their complaint has been dealt, they will have the right to complain to the ICO. The DPO will inform the complainant about their right to complain to the ICO.
- The DPO will record the complaint in the Activities and Incident Log. These records will be stored for 7 years.

If the complainant decides to raise the issue with the ICO, the DPO will coordinate with the ICO in the investigation.

23. Links with Other Policies

This data protection policy is linked to our:

- Appropriate Policy Document
- Privacy Notice
- Data Retention Policy and Schedule
- Legitimate Interest Assessment
- Record of Processing Activities
- Subject Access Request
- Business Continuity Plan
- Safeguarding Policy
- Safeguarding Code of Conduct
- Complaints Policy

Appendix 1 Personal data breach procedure

Article 4.12 of the UK GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, authorisation, and authorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost.
- Stolen.
- Destroyed.
- Altered.
- Disclosed or made available where it should not have been.
- Made available to unauthorised people.

- The SIRO will alert the Chair of Trustees.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, they will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or nonmaterial damage (e.g., emotional distress), including through:
  - Loss of control over their data.
  - Discrimination.
  - Identify theft or fraud.
  - Financial loss.
  - Unauthorised reversal of pseudonymisation (for example, key-coding).
  - Damage to reputation.
  - Loss of confidentiality.
  - Any other significant economic or social disadvantage to the individual(s) concerned.

  Mitigating factors that may be considered when not reporting a breach include:

  - the data is retrievable.
  - there is evidence that data has been contained and that those who may have access will not process the data in such a way as to cause harm or distress to the data subjects concerned.

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored in the Data Protection file kept at the organisation's registered address.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, they will set out:

A description of the nature of the personal data breach including, where possible:

  - The categories and approximate number of individuals concerned.
  - The categories and approximate number of personal data records concerned.
  - The name and contact details of the DPO.
  - A description of the likely consequences of the personal data breach.
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. They will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, they will communicate the breach without undue delay to the affected individuals. In some circumstances, the organisation may decide to not inform the individuals if by doing so it would cause more damage to the data subjects than the data breach itself.
- This notification will set out:
  - The name and contact details of the reporting person (DPO).
  - A description of the likely consequences of the personal data breach.
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

  If the individuals are informed of the data breach, the organisation will also ask if they want to log a formal complaint to the ICO regarding how their personal data has been managed.

  The agreements that the organisation stipulates with data processers includes a clause requiring them to inform the organisation immediately, or in any event within 24 hours of them becoming aware of a breach. This is to allow the organisation to make a report to the ICO within the 72 hours.

  If a data subject has been harmed by a breach of data protection legislation, they can take the controller to court for compensation. Contractors, subcontractors and other parties may be subject to appropriate legal action in accordance with the organisation's processing agreement. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred immediately to the relevant authorities.

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies.

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause.
    - Effects.
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored in the Data Protection file kept at the organisation's registered office.

- The DPO/SIRO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The organisation will take the actions set out below to mitigate the impact of different types of data breaches, with particular focus on those involving high-risk or sensitive information. The effectiveness of these actions will be reviewed following any data breach and updated as necessary.

Sensitive information being disclosed via email (including safeguarding records):

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to take corrective action as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- In all cases, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save, or replicate it in any way.
- The DPO will ensure that written confirmation is obtained from all individuals who received the data, verifying that they have complied with the request.

Non-anonymised data relating to service users/staff being shared with Trustees.

- If non-anonymised data is shared with Trustees, the supplier of the data must attempt to take corrective action as soon as they become aware of the error.
- Trustees who receive non-anonymised data must alert the supplier and the DPO as soon as they become aware of the error.
- If the data has been sent via email, the corrective action relating to the disclosure of sensitive information via email will be followed.
- If the data has been issued in hard copy, the supplier of the information will i) retrieve all copies and ensure they are destroyed securely; ii) or ask the trustees to destroy the data securely.

The DPO will ensure we receive a written response from the Trustees confirming that they have deleted the data securely, (or returned it to the supplier) and have not shared, published, saved or in any way replicated the data.