No. 20a Data Protection Policy

Version Number	Amendments Made	Date
1	Use of CCTV added to Section 12 Whole Policy Updated into new template Links with other policies updated Use of Multifactor Authentication added in section 15	06/10/24
2		

Approved by	Brendan Dunphy
Date of Issue	October 2024
Review due (date)	October 2025

Contents

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 General Data Protection Regulation (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 GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the 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.

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.

7.2. Senior Information Risk Owner/Data Protection Champion

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

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 Champion (DPC, Clinical Manager) is the first point of contact for individuals whose data the Organisation processes, and the SIRO is the first point of contact for the Information Commissioner's Office (ICO: https://ico.org.uk) in this case. The SIRO is responsible for reporting all other data breaches.

Full details of the Data Protection Champion's responsibilities are set out in their job description.

The Lowdown's Senior Information Risk Owner is:

Sharon Womersley (CEO) sharonwomersley@thelowdownnorthampton.co.uk

The Lowdown's Data Protection Champion is:

Rachel Welsh (Clinical Manager) rachelwelsh@thelowdownnorthampton.co.uk.

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 DPC/SIRO 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.
- 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 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

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- 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.

If we offer services to young people under 13, we will get parental consent.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

9.2. Limitation, Minimisation, and Accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

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

We will not normally share personal data with anyone else, but may do so 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.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and service users – for example, IT companies. When doing this, we will:
    - 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.

We will also share personal data with law enforcement and government bodies where we are legally required 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.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our service users or staff.

11. Subject Access Requests and Other Rights of Individuals

11.1. Subject Access Requests

Individuals have a right to make a 'subject access request' 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 must be submitted in writing, either by letter or email to the DPC. 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 DPC.

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 at The Lowdown 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, we:

- 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.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if 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 the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

11.4. Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 9), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us 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).

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

12. CCTV

We use CCTV in various locations around The Lowdown's sites to ensure clients, staff and visitors are safe. We adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Lisa Braithwaite, Office Manager.

13. Photographs and Videos

As part of The Lowdown's activities, we may take photographs and record images of individuals.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and service user if under 18.

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 can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot 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

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPC, and ensuring they have 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 DPC 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; we will also keep a record of attendance.
- 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.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of The Lowdown and DPC and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and 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.
- 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 (see our Acceptable use agreement);
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 10).

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the organisation's behalf. If we do so, we will require the third party to provide sufficient guarantees that it 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, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the 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.e-lfh.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.

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. Links with Other Policies

This data protection policy is linked to our:

- Confidentiality and Information Sharing Policy
- Data Security Policy
- Data Quality Policy
- Privacy Notice Employees
- Privacy Notice Students and Volunteers
- Privacy Notice Service Users' Policy
- Record Keeping Policy
- Document Retention Policy
- Business Continuity Plan
- Privacy Policy
- Safeguarding Policy

21. Appendix 1

Appendix 1: Personal data breach procedure

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 DPC/SIRO.
- The DPC/SIRO will investigate the report and determine whether a breach has occurred. To decide, the DPC 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 DPC 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 DPC will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPC/SIRO 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 non-material 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

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

- The DPC/SIRO will document the decision (either way), in case it is challenged at a later date 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 DPC/SIRO 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 DPC/SIRO
- 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 DPC/SIRO 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 DPC/SIRO 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 promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the reporting person (DPC/SIRO)
  - 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.
- The DPC/SIRO 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 DPC/SIRO 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.

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

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 DPC as soon as they become aware of the error.
- In all cases, the DPC 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 DPC will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this 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 DPC/SIRO 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 DPC/SIRO 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.