Last updated: June 2025
We are committed to reviewing and updating our policies every 2 years.
Review due: June 2027

Data Protection Policy

This policy is intended to cover the Data Protection responsibilities of Common Room North Ltd towards those who work for and with us.

1. Background

The UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (DPA 2018)outline the national regulations for the processing of information relating to individuals. This includes the obtaining, holding, using or disclosing of this information, and covers computerised records as well as paper filing systems.

Data users must comply with the data protection principles of good practice which underpin the UK GDPR and DPA 2018. Personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
- **Accountability:** The controller shall be responsible for, and be able to demonstrate compliance with, the above principles.

It is the policy of Common Room North Ltd that all personal data will be held in accordance with the principles and requirements of the UK GDPR and DPA 2018, and other relevant legislation. Procedures will be put in place to ensure the fair processing of data subjects. Liz Neill, Director and Information Governance Lead, is responsible for overseeing compliance with this policy. All Common Room North Ltd employees will work with Liz Neill to ensure Data Protection procedures are adhered to.

Relevant data protection issues will be included in all induction and ongoing training.

2. Lawful Basis for Processing Personal Data

Under UK GDPR, Common Room North Ltd must have a valid lawful basis for processing personal data. We rely on the following lawful bases for different types of processing activities:

- **Contractual Necessity:**

    - **Purpose:** To fulfil our contractual obligations with individuals (e.g., employees, contractors) and partner organisations (e.g., delivering specific project outcomes as agreed).
    - **Examples:** Processing employee payroll, managing project deliverables as agreed in a service level agreement, contacting individuals regarding their participation in a contracted work project.
- **Legal Obligation:**
    - **Purpose:** To comply with a legal or regulatory obligation.
    - **Examples:** Sharing information with HMRC for tax purposes, complying with safeguarding duties, responding to lawful requests from law enforcement, maintaining statutory records.
- **Legitimate Interests:**
    - **Purpose:** Where processing is necessary for our legitimate interests or those of a third party, provided these interests do not override the fundamental rights and freedoms of the data subject. We conduct a Legitimate Interests Assessment (LIA) to ensure this balance.
    - **Examples:** Internal administrative purposes, ensuring network and information security, for the establishment, exercise or defence of legal claims, general communications with partner organisations about non-contractual collaboration opportunities, improving our services, managing internal complaints.
- **Consent:**
    - **Purpose:** Where individuals have given clear, affirmative consent for us to process their personal data for a specific purpose. Consent will always be freely given, specific, informed, and unambiguous. Individuals have the right to withdraw their consent at any time.
    - **Examples:** Using photographs or recordings for promotional purposes, sending marketing communications (where not covered by legitimate interest and soft opt-in rules for existing customers), processing certain sensitive personal data for non-essential purposes where no other lawful basis applies.
- **Vital Interests:**
    - **Purpose:** To protect an individual's life. This is typically used in emergency situations.
    - **Examples:** Sharing medical information with emergency services if an individual is incapacitated and at risk of harm.

Special Category Data: When processing 'special category' personal data (e.g., health information, ethnicity, religious beliefs, sexual orientation), we ensure an additional condition for processing (from UK GDPR Article 9) is met. This often includes explicit consent, substantial public interest (with a basis in law), or where necessary for reasons of substantial public interest (e.g., for equal opportunities monitoring, with appropriate safeguards and anonymisation).

3. Data Subject Rights

Under the UK GDPR, individuals have specific rights regarding their personal data. Common Room North Ltd is committed to upholding these rights. You have the right to:

- **Right to be Informed:** To be informed about how and why your personal data is being processed (as provided by this policy and our data protection statement).
- **Right of Access (Subject Access Request - SAR):** To request a copy of the personal data we hold about you.
    - **How to make a SAR:** Requests should be made in writing (email) and addressed to Liz Neill, Director and Information Governance Lead

(Liz.Neill@commonroom.uk.com). We may ask for proof of identity to ensure we only share data with the correct person.
    - **Response Time:** We will respond to your SAR within **one calendar month** of receiving your request. This period may be extended by a further two months if the request is complex or numerous, in which case we will inform you of the extension and the reasons for it within the initial one-month period.
    - **Charges:** We will provide your data free of charge. However, we may charge a reasonable fee for requests that are clearly unfounded, excessive, or repetitive, or if you request further copies of the same information. In such cases, we will inform you of the fee and the reasons for it.
- **Right to Rectification:** To request that inaccurate or incomplete personal data we hold about you is corrected without undue delay.
- **Right to Erasure ('Right to be Forgotten'):** To request the deletion or removal of personal data where there is no compelling reason for its continued processing. This right is not absolute and only applies in certain circumstances.
- **Right to Restriction of Processing:** To 'block' or suppress the processing of your personal data in certain circumstances (e.g., if you contest its accuracy or object to its processing). This means we can store your data but not use it.
- **Right to Data Portability:** To obtain and reuse your personal data for your own purposes across different services. This right applies to data you have provided to us, which is processed by automated means, and where the processing is based on consent or a contract.
- **Right to Object:** To object to the processing of your personal data in certain situations, particularly where it is based on legitimate interests or for direct marketing purposes.
- **Rights in relation to automated decision-making and profiling:** To not be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you, unless certain exceptions apply. Common Room North Ltd does not currently engage in automated decision-making or profiling that would have significant effects.

Making a Complaint to the ICO: If you are unhappy with how Common Room North Ltd has handled your personal data, you have the right to complain to the Information Commissioner's Office (ICO), the UK's independent authority for data protection.

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline: 0303 123 1113
Website: www.ico.org.uk

4. Data Breach Procedure

Personal Data Breach Management

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Common Room North Ltd has procedures in place to detect, report, and investigate any personal data breaches.

Our Procedure:

1. **Identification:** All staff are trained to identify and immediately report any suspected personal data breach to Liz Neill, Director and Information Governance Lead.
2. **Assessment:** Upon notification, Liz Neill will promptly assess the reported incident to determine if it constitutes a personal data breach and to establish the risk to individuals.
3. **Containment and Recovery:** Immediate steps will be taken to contain the breach, minimise its impact, and recover any lost data.
4. **Notification to ICO:** If the breach is likely to result in a **high risk to the rights and freedoms of individuals**, we will report it to the Information Commissioner's Office (ICO) without undue delay, and no later than **72 hours** after becoming aware of it.
5. **Communication to Affected Individuals:** If the breach is likely to result in a **high risk to the rights and freedoms of individuals**, we will also communicate the breach to the affected individuals without undue delay. This communication will clearly explain the nature of the breach, the likely consequences, and the measures taken or proposed to address it.
6. **Investigation and Learning:** A thorough investigation will be conducted to determine the cause of the breach and to identify and implement measures to prevent recurrence. All breaches are recorded internally for accountability and learning purposes.

5. Data Processors

Third-Party Data Processors
Common Room North Ltd sometimes uses third-party organisations (Data Processors) to process personal data on our behalf (e.g., cloud storage providers, payroll services, CRM systems). When we engage a Data Processor, we remain the Data Controller and are responsible for the personal data.

Our Commitment to Data Processor Management:

- We will only use Data Processors who can provide sufficient guarantees that they will implement appropriate technical and organisational measures to meet the requirements of the UK GDPR and protect the rights of data subjects.
- We will ensure that a legally binding **written contract (Data Processing Agreement)** is in place with every Data Processor. This contract will specify the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of Common Room North Ltd as the controller.
- The contract will include provisions that require the Data Processor to:
    - Only process personal data on documented instructions from Common Room North Ltd.
    - Ensure that persons authorised to process the personal data are committed to confidentiality.
    - Implement appropriate security measures.
    - Assist Common Room North Ltd in meeting its GDPR obligations regarding data subject rights and security.
    - Return or delete all personal data at the end of the service.
    - Allow for audits and inspections.
    - Inform Common Room North Ltd of any sub-processors they intend to use.

6. Accountability and Governance

Common Room North Ltd demonstrates its compliance with UK GDPR through the principle of accountability. This means we are responsible for, and can demonstrate, our compliance with all data protection principles.

Our approach to accountability includes:

- **Information Governance Lead:** Liz Neill, Director, is our designated Information Governance Lead, responsible for overseeing data protection compliance.
- **Records of Processing Activities (ROPA):** We maintain accurate and up-to-date records of our data processing activities, detailing:
    - The purposes of the processing.
    - The categories of data subjects and personal data.
    - The categories of recipients to whom the personal data has been or will be disclosed.
    - Where possible, the envisaged time limits for erasure of different categories of data.
    - A general description of the technical and organisational security measures.
- **Data Protection Training:** All staff receive regular training on data protection principles, their responsibilities, and our policies and procedures.
- **Policy Review and Updates:** This Data Protection Policy and related procedures are regularly reviewed and updated (at least every two years, or sooner if there are legislative changes or changes to our processing activities) to ensure ongoing compliance.
- **Privacy by Design and Default:** We incorporate data protection considerations into the design of new projects, systems, and processes, ensuring that data protection is built in from the outset and that only necessary data is processed by default.
- **Data Protection Impact Assessments (DPIAs):** We conduct DPIAs for any new projects or processing activities that are likely to result in a high risk to the rights and freedoms of individuals. This process helps us identify and mitigate data protection risks before they materialise.
- **Internal Audit and Monitoring:** We regularly monitor our data processing practices and compliance with this policy.

7. Data Retention Schedule

Data Retention

Common Room North Ltd retains personal data only for as long as is necessary to fulfil the purposes for which it was collected, or as required by law or contractual obligations. This is in line with the UK GDPR principle of 'storage limitation'.

- **General Principle:** Information no longer required will be disposed of appropriately and securely (e.g., shredding paper records, secure deletion of digital files).
- **Retention Schedule:** We maintain a **Data Retention Schedule** (available upon request from the Information Governance Lead) which specifies the retention periods for different categories of personal data we process. This schedule is based on legal requirements, industry best practices, and our business needs.
    - **Examples from our Retention Schedule include (but are not limited to):**
        - **Employee Records:** Retained for 5 years after employment ends, to meet legal obligations related to tax, national insurance, and potential claims.
        - **Project Participant Data:** Retained for the duration of the project plus 2 years for evaluation, reporting, and safeguarding purposes, then securely deleted.
        - **Financial Records:** Retained for 6 years plus the current financial year, as required by HMRC.
        - **Safeguarding Records:** Retained in line with statutory guidance (e.g., until the child reaches 25, or for specific periods depending on the nature of the concern).
        - **Marketing Consent Records:** Retained for as long as consent is active, plus a short period after withdrawal to demonstrate compliance.

Information held by Common Room

- Liz Neill, Director, is the appointed Information Governance Lead.
- Information held by Common Room relates to organisations who we provide services to and work alongside, and individuals (including employees, attendees at Common Room events and workshops and young people or other stakeholders we have an ongoing relationship with)
- Common Room will ensure that individuals know enough about how information held about them is used or disclosed, by sharing and explaining the *Common Room Data Protection Statement*. (see page 7 of this policy). Information held about individuals will only be collected and recorded with good reason. It will be stored securely and for only as long as required.
- Relevant data protection issues will be included in all induction and training of staff.
- Common Room will not give out information about any individual over the telephone or by e-mail unless it is satisfied that the individual knows that this type of disclosure may be made and/or the information is already in the public domain (or that there is an overriding reason for the disclosure such as safeguarding the wellbeing of a child, young person or vulnerable adult).
- No details of individuals will be passed to other organisations for marketing, fundraising or circulating information unless consent has been obtained and the individual given the opportunity to opt-in or opt-out.
- Photographs and recordings of film or audio, in which any children or young people (under 16 years of age) can be identified will only be used with explicit written consent from parents or guardians.
- Any documents containing contact information about children or young people are to be password protected and passwords stored separately. Computer files containing sensitive information about individuals will be password protected, accessible only to relevant staff and the Director.
- Information no longer required will be disposed of appropriately.
- Paper files containing sensitive information about individuals will be kept in locked filing cabinets, accessible only to relevant staff and the Director. Paper files will be kept to a minimum.

Staff records

- The names and posts held by staff within Common Room, including Common Room Employees, are considered to be in the public domain and may be made freely available in any format to anyone.
- All information required for the purposes of payroll is confidential and made available only to the Finance Manager and Director. Information will be passed to statutory bodies if a legal requirement, such as in connection with tax and national insurance.
- All other information within staff records is confidential. Personnel records are only used for matters connected with the individual's employment at Common Room or to help with references Common Room might write in future at the individual's request.
- Staff will be given full open access to their complete personnel records without question and without charge. Staff can request this via the Director.

Documents containing information about individuals working with Common Room

- Documents containing information about individuals (including children and young people) shall be confined to information directly relevant to the reason for their involvement with the work of Common Room. Name, home address, phone number and details of an emergency contact will be collected for the purposes of safeguarding individuals who work with

Common Room. This data will be accessible during events and projects, password protected in digital files.

- Information about gender, ethnicity and disability of individuals will be kept anonymous and is collected only for the purposes of monitoring equal opportunities and reporting back to funders.
- Data about individuals will be deleted on the request of the individual and/or when the data is no longer used or required by Common Room.
- Data about individuals will only be used by Common Room for; sharing information about current work projects and opportunities, safeguarding individuals, providing contact details for a specified organisation when requested or any other reason which has been specifically agreed with individuals in advance.

The following statement will be used on all external forms used to gather information that is kept by Common Room.

Common Room North Data Protection Statement

Common Room North takes your privacy seriously. We collect and process your personal information to deliver our projects and services, and to comply with legal obligations (like safeguarding).

Your data is kept securely, only accessible internally on a need-to-know basis, and retained only for as long as necessary. We won't share your information with external parties without your permission, unless there's a legal requirement or a specific safeguarding concern.

You have rights over your data, including the right to access it and ask for corrections.

Read our full **Data Protection Policy** and **Safeguarding Policy** for more details.