# GRCC Data Protection and Information Governance Policy

## Document Information:

| | |
|---|---|
| Document reference: | Data Protection and Information Governance – Policy number 4 |
| Date first issued: | August 2007 (as Data Protection and Confidentiality Policy) |
| Date due for review: (if applicable) | May 2026 |
| Network location: | Z:\Quality Standards\GRCC POLICIES & PROCEDURES\4 Data Protection + Info Governance\Policy |
| Owner: | SLT |
| Date of Governance Committee scrutiny: | 15 November 2024 |
| Date of last adoption by Board of Trustees: (if applicable) | 27 October 2025 |
| Related documents: | *1. Health and Safety Policy & Procedures; 3. Information Technology and Communications Policy; 7. Induction Policy & Process for New Staff; 8. Induction Policy & Process for New Trustees; 9. Volunteer Policy; 16. Finance Policy; 20. Confidentiality Policy*<br>*Employee Handbook (esp. Disciplinary and Grievance Policies)*<br>*GRCC Business Continuity Plan* |

## Version number, date and amendment history

| Version Number | Date of review / amendment | Amended by: | Section, page, text amended: |
|---|---|---|---|
| v.17 | December 2025 | BPi / BPo / CH | Updated to include recording, storage, and publication of staff and volunteer photos |
| v.16 | October 2025 | BPi / BPo / CH | Additions relating to use of AI; updated Related Documents section |
| | March 2024 | CH | Formatting and punctuation corrections; updated Related Documents section; removal of references to Independence Trust. Version number unchanged |
| | November 2022 | CH / BPo | Joint branding; minor clarification re public WiFi. Version number unchanged |

| | | | |
|---|---|---|---|
| v.15 | July 2022 | CH | Addition of cyber security training reference to section 12; amendment re staff use of own devices; subject access requests added to data retention period |
| | June 2021 | CH | Minor alterations only – correction of typing errors. Version number not changed |
| v.14 | August 2020 | CH / SLT | Section 1: clarification of legislation<br>Section 5: addition of waste disposal methods<br>Section 10: change to timing of audit of practice<br>Amended policy adopted by BoT 27/10/2020 |
| v.13 | January 2020 | CH | Section 6: updated details of data controller / ICO contact |
| v.12 | Dec 2019 | ET | Amendments to Section 12- Data Security re new IT Cloud system |
| | May 2019 | | Reviewed May 2019 – no changes made |
| v.11 | October 2018 | HL | Rebranding |
| v.10 | 8 June 2018 | SLT | • Amendments following Board of Trustees input.<br>• Altered to reflect new GRCC structure<br>• Addition of lawful reasons for processing |
| v.9 | May 2018 | SMT | • Reviewed and amended to make GDPR compliant<br>• Change of title |
| v.8 | February 2017 | | • Incorporating wording from previous versions of the Employee Handbook into the policy introduction<br>• Additional information re Information Sharing Agreements |
| v.7 | July 2016 | | • Corrected font sizes and typing errors<br>• Changed reply form return details |
| v.6 | December 2015 | | |
| v.5 | October 2014 | | |
| v.4 | 2013 | | |
| v.3 | 2011 | | |
| v.2 | 2009 | | |
| v.1 | August 2007 | | |

# 1. Aims of the Policy

GRCC needs to keep certain information on its employees, clients, service users, Trustees and volunteers to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 2018 incorporating the General Data Protection Regulations (GDPR) 2018. These are concerned with the processing of computerised and manual information about living individuals (personal data) by GRCC. Organisations are required to demonstrate compliance, including the ongoing confidentiality, integrity, and availability of data and the resilience of processing. Individuals who are the subject of that information are conferred with rights.

GRCC will comply with the law, collecting and using personal information fairly and with transparency, storing it safely and disposing of it in a timely, safe manner.

The aim of this policy is to ensure that everyone handling personal data at GRCC is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation to ensure compliance and accountability.

This policy covers employed staff, Trustees, volunteers and clients / service users.

GRCC is a Data Controller. The organisation may also be a Data Processor for other organisations.

# 2. Definitions

**Personal data** - Any information relating to an identifiable, living person who can be directly or indirectly identified through the data held. Examples are name (including name within an email address), identification number, location data, and images (e.g., pictures and videos of employees, Trustees, and volunteers). The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

**Processing** - anything that is done to or with the data, whether in hard copy or electronic form.

Lawful basis for processing:

**(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

**(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

**(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

**(d) Vital interests:** the processing is necessary to protect someone's life.

**(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

**Data Controller and Data Processor -** A controller determines the purposes and means of processing personal data whereas a processor is responsible for processing personal data on behalf of a controller. The controller is responsible for, and should be able to demonstrate, compliance with the principles.

**Special category data** relates to race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

## 3. Principles

The seven principles of GDPR lie at the heart of GRCC's approach to processing personal data:

- Lawfulness, fairness and transparency – Data is processed lawfully, fairly and in a transparent manner in relation to individuals.
- Purpose limitation – Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data minimisation – Data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Accuracy – Data is accurate and, where necessary, kept up to date, ensuring that inaccurate personal data is erased/ rectified without delay.
- Storage limitation – Data is kept for no longer than is necessary.
- Integrity and confidentiality (security) – There is 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.
- Accountability – the controller is responsible for, and able to demonstrate compliance with the above 6 principles.

## 4. Identifying the type of information processed

GRCC conducts an information audit on a half yearly basis, or as project changes occur. This provides an Information Asset Register, showing flows and usage of personal information held by GRCC and identifying the lawful basis for processing, including legitimate interests.

In general, the following types of information are processed:

| Types of information | Lawful basis for processing |
|---|---|
| Trustees' information – contact details, eligibility to serve and declarations of interest plus notes of meetings, photograph (for ID if applicable and (with permission) for use on organisation website, social media, and any other marketing materials for external use). | Legal obligations - e.g., Charity Commission and Companies House compliance<br><br>Legitimate interests - record keeping of meetings.<br><br>Consent – use of photograph; consent for the use of photographs can be withdrawn at any time, including once a Trustee has stood down from the Board |
| Information on applicants for posts, including references where applicable | Legitimate interests - to aid recruitment process.<br><br>For any special category information regarding disability – legitimate interests – to enable reasonable adjustments for interview, where applicable. |
| Employee information consistent with the employment relationship – references obtained during recruitment, details of terms of employment, job duties, contact names and addresses including next of kin, bank account number, payroll information, tax and national insurance information, health and sickness absence records, holiday records, evidence of valid driving license and vehicle insurance (if applicable), DBS check reference numbers (if applicable), photograph for ID and (with permission) use on organisation website, social media and any other marketing materials for external use, information about performance, supervision and appraisal notes, details of any disciplinary investigations and proceedings (if applicable), training records, correspondence with GRCC and other information provided to GRCC including, where applicable, accident records | Legal obligations - e.g., processing information relating to right to work in the UK, pension and HMRC requirements.<br><br>Contractual - processing in relation to terms and conditions of employment.<br><br>Legitimate interests- to enable effective support and supervision record keeping.<br><br>Consent – use of photograph; consent for the use of photographs can be withdrawn at any time, including once an employee has left employment at GRCC<br><br>Special category information relating to health (where applicable) - Legitimate Interests- to enable effective support and supervision. Legal and contractual – to demonstrate compliance with contract of employment and employment law. |
| Volunteer information – application form, references obtained during recruitment, contact details, bank account number, evidence of valid driving license and vehicle insurance (if applicable), DBS check reference numbers (if applicable), support meeting | Legitimate interests- to enable effective support and supervision.<br><br>Legal obligations- e.g., compliance with HMRC re expenses payable. |

| | |
|---|---|
| notes, photograph (for ID if applicable and (with permission) for use on organisation website, social media, and any other marketing materials for external use). | Consent – use of photograph; consent for the use of photographs can be withdrawn at any time, including once a volunteer has left their role with GRCC |
| Members – contact details, bank account details (if applicable), membership payment details | Legal obligations - to enable compliance with governing document (e.g., AGM notice)<br><br>Legitimate interests – to enable record keeping of contact, activity and payment. |
| Service users – contact details, notes in relation to project / activity progress, bank account details (of payments made for courses). Some GRCC projects require processing of personal sensitive information about individuals supported by our projects, including notes about issues and the support provided. (Some of these may be special category data, therefore the lawful basis for the special category data must be specified.) | Legitimate interests - to enable effective advice and support.<br><br>Contractual - to demonstrate delivery against contracts, and to enable records of consultancy services provided.<br><br>Consent - for processing in relation to GRCC marketing information.<br><br>Where specific projects process special category information or the lawful basis for processing differs to the above, the lawful basis for processing will be clarified on data capture or agreement forms. |

Personal information is kept in electronic and hard copy reference files. Some personal information is transferred electronically or stored on websites.

Groups of people within the organisation who will process personal information are GRCC-employed staff and GRCC volunteers, including Trustees.

## 5. Retention Periods

The following guidelines are followed in relation to retention periods:

| Record | Retention period |
|---|---|
| Personnel files | 6 years after employment / volunteering ceases, (slimmed down (redacted) format after 2 years including DBS check documents and status) |
| Application forms and interview notes (unsuccessful candidates) | 6 months following application process closure |
| Letters of reference | 6 years from the end of employment |
| Redundancy details | 6 years from the date of redundancy |
| Parental leave | 5 years from birth/adoption or 18 if child receives a disability allowance |

| | |
|---|---|
| Assessments under health & safety regulations | Permanently |
| Accident books, accident records/reports | 3 years |
| Income tax, NI returns, income tax records and correspondence with IR | At least 3 years after the end of the financial year to which they relate |
| Statutory maternity / paternity pay records and calculations | At least 3 years after the end of the financial year to which they relate |
| Statutory sick pay records and calculations / compassionate leave | At least 3 years after the end of the financial year to which they relate |
| Wages and salary records | 6 years |
| Employee joining / new starter form | 6 years after employment ceases |
| Project information on service users | Data relating to programmes will be retained for as long as is necessary to provide an audit trail for funders, as set out in contractual agreements. For European Funded projects this can be up to 13 years. |
| Subject Access Requests | Statutory retention period: 1 year following completion of the request. |

Data in hard copy will be shredded and / or disposed of through a confidential waste contractor. Staff or volunteers must only dispose of paper records containing personal data at GRCC premises using the shredding machine. Electronic data will be deleted from the server.

## 6. Registration with the Information Commissioner's Office

Our requirements for processing personal data are recorded on the public register maintained by the Information Commissioner' Office (ICO). We notify and renew our notification on an annual basis as the law requires. If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

GRCC is a Data Controller and the link person between GRCC and the Information Commissioner's Office is Russell Hayward (russellh@grcc.org.uk). A copy of the certification is on display on the Community House noticeboard.

## 7. Responsibilities

Overall responsibility for personal data at GRCC rests with the Board of Trustees which delegates operation to the Senior Leadership Team and the Data Protection Lead who is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures to demonstrate compliance and accountability
- auditing GRCC practice to ensure compliance, and taking measures as necessary
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes
- investigating any breaches of the policy within the organisation

All employed staff, Trustees and volunteers who process personal information have a responsibility to abide by the policy. They must ensure they understand and act in line with this policy and the data protection principles, including completing mandatory cyber security training. Any queries are to be immediately raised with line managers and any concerns about breaches are to be brought to the attention of line managers, who will inform the Senior Leadership Team and Data Protection Lead.

GRCC is accountable to its service users, funders and ultimately to the Information Commissioner in relation to data protection legislation. We aim to support staff and volunteers to abide by this policy but serious breaches by employed staff could result in disciplinary proceedings, or in the case of volunteers, in the termination of the volunteering agreement.

The Board of Trustees is accountable for compliance with this policy. A Trustee could be personally liable for any penalty arising from a breach that they have made.

## 8. Policy Implementation

To meet our responsibilities GRCC will ensure that:

- An Information Asset Register is maintained – an analysis of data held across the organisation
- The GRCC Privacy Notice is GDPR compliant and available to data subjects. It will clearly contain the necessary information, as set out in the GDPR, in plain English:
    - Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer
    - Purpose of the processing and the lawful basis for the processing
    - The legitimate interests of the controller or third party, where applicable
    - Categories of personal data
    - Any recipient or categories of recipients of the personal data
    - Details of transfers to third country and safeguards
    - Retention period or criteria used to determine the retention period
    - The existence of data subject's rights:
        - The right to withdraw consent at any time, where relevant
        - The right to lodge a complaint with a supervisory authority

    - The source the personal data originates from and whether it came from publicly accessible sources (not relevant if data supplied directly by the subject)
    - Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
    - [Not applicable to GRCC - The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences]

- Provide data capture form templates for staff
- Ensure marketing information is only sent to individuals on the basis of consent and GRCC has systems in place to manage ongoing consent – i.e., a log, managed by a named member of GRCC staff
- Everyone managing and handling personal information is trained to do so
- Any disclosure of personal data will be in line with GRCC procedures
- Line managers support employed staff and volunteers with any data protection queries or concerns
- Ensure the rights people have in relation to their personal data can be exercised
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, is informed about the processes involved
- Subject Access requests (queries about handling personal information) will be dealt with within the timescales required in the GDPR, and the process for individuals to make a request will be clear
- Log and investigate any breaches of this policy, put measures in place to avoid further incidents and inform the ICO as appropriate.
- Require organisations and individuals who are Data Processors for GRCC to confirm the measures in place to comply with regulations, thereby protecting the integrity of the data and preventing unauthorised access

Employed staff, volunteers and Trustees will:

- Collect personal data in a fair and lawful way
- Use GRCC templates for data capture forms and make available additional information to supplement the Privacy Notice, as required
- Record the date and name of person capturing the information, if information is captured orally
- Make available the privacy notice and any additional information at point of data collection or within 1 month of a referral (or at first point of contact if earlier)
- Explain why data is needed at the start, including the lawful basis for processing the data
- Identify the lawful basis for processing any special category information, taking advice from managers

- Ensure that only the minimum amount of information needed is collected and used, including in relation to AI within the parameters of the Information Technology and Communications policy and procedure
- Ensure the information used is up to date and accurate, amending records as necessary
- Review the length of time information is held
- Ensure it is kept safely
- Dispose of confidential information securely
- Raise queries about data protection and concerns about possible breaches (immediately) with line managers, who will, in turn, inform the Senior Leadership Team and Data Controller
- Pass on enquiries for subject access immediately to their line manager / Senior Manager
- Provide data to answer subject access requests promptly
- Keep managers informed of any organisations / individuals who are Data Processors on behalf of GRCC.

## 9. Training

Training and awareness raising for employed staff, Trustees and volunteers about the Data Protection Act and how it is followed in this organisation will take the following forms:

### On induction:

- Provision of the Data Protection and Information Governance Policy and key procedures. Guidelines on common breaches and how to avoid them are provided
- Specific instructions are provided for data security, including when working from home or out in the community, using mobile equipment and during online access to GRCC systems. Public WiFi should never be used to access GRCC systems
- Specific instructions are provided for secure email usage, as appropriate
- Discussion with line manager to ensure understanding of policy, procedure and GRCC practice.
- New members of staff and volunteers are required to sign for information received as proof of receipt and understanding.
- New members of staff, volunteers and Trustees are required to undertake mandatory cyber security training and training on the use of AI.

### General training / awareness raising:

- Annual refresh training for staff during team meetings, referring to GRCC policies and procedures
- Cyber security training
- Periodic reminders of how to avoid common breaches of GDPR

- Line manager meetings with staff and volunteers to include discussion and audit of practice in relation to data processing
- Employed staff and volunteers are required to raise any queries about data protection and any concerns regarding possible breaches with line managers/ supervisors
- Half yearly audit of procedures and practice

## 10. Gathering and checking information

Before personal information is collected, GRCC will utilise a 'privacy by design' methodology, considering:

- The personal details necessary for the purposes of the project or activity
- The lawful basis for processing the information, including legitimate interests
- Where special category information is to be gathered, the lawful basis for gathering the information
- Whether the information will be passed on to a third party, and if so, to whom
- How long this information will be needed
- Where risk is higher (due to the nature of the data held or the transfer or sharing of data) and conducting an Impact Assessment in these cases

We will inform people whose information is gathered about the following:

- why the information is being gathered
- what the information will be used for
- who will have access to their information (including third parties)

In the majority of cases this will be outlined through a data capture statement on the form to be completed, linking to the GRCC Privacy Notice. Oral data capture statements may also be used. In some cases, we will ask service users to confirm they understand how the data will be used, especially if there is a possibility of sharing data with other organisations.

We will take the following measures to ensure that personal information kept is accurate:

- Checking and validation processes to ensure accuracy on data input
- Annual audit of practice and data held on individuals (including service users, partners and other stakeholders)
- Requesting employed staff and volunteers to notify GRCC of any changes to personal details
- Adjusting records in a timely manner when informed of a change or inaccuracy, for employees, volunteers, trustees, members, service users and other stakeholders

## 11. Information Sharing Agreements

GRCC Managers will identify when Information Sharing Agreements are required in project areas and staff / volunteers involved in delivery of those projects will be made aware of the contents of the agreement.

The Information Sharing Agreement will identify and clarify aspects such as:

- Individual users' rights such as consent
- Access to information
- Data collection tools/ forms
- Requirements for certified true copies of documents
- Accepted security standards and secure records storage and retention
- Transfer of information (e.g., use of secure email systems)
- Privacy Notice/ Statement / Policy, subject access requests, Freedom of Information, Records Management, Information security requirements, processes for dealing with concerns and complaints
- Restrictions around the use of AI tools in relation to projects

## 12. Data Security

GRCC will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures are taken:

- Using lockable cupboards (restricted access to keys)
- Password protection or restricted access to personal information files
- Restricted access to areas of the GRCC computer system
- Restricted access to website login areas
- Instructions are provided for staff and safe keeping of any personal data taken off site in hard copy or electronically (e.g., on a mobile device or laptop). Public WiFi should not be used to access GRCC systems
- Staff working from home using their own equipment are only permitted to work through the remote access hosted desktop.
- Safe storage of electronic information through ICT provider
- Password protected attachments for sensitive personal information sent by email, if not sent via secure email
- Checking understanding and, if necessary / appropriate, gaining permission before disclosing personal information (including personal contact details)
- No disclosure of personal data to a third party without making this clear to the data subject
- Contractors (e.g., IT contractors and other data handlers) who are data processors for GRCC and have access to GRCC data will be required to have measures in place to protect the integrity of the data and prevent unauthorised access

- When employees / volunteers with access to IT systems leave GRCC relevant passwords / access rights, including remote access rights, are immediately amended.

Any unauthorised disclosure of personal data to a third party by a GRCC employee without following due process may result in disciplinary procedures. Any unauthorised disclosure made by a volunteer or Trustee may result in the termination of the volunteering agreement. Unauthorised disclosures or breaches by Data Processors for GRCC may result in end of contract and / or reporting the organisation to the ICO and end of contract.

## 13. Individual Rights and Subject Access Requests

The GDPR provides the following rights for individuals:

- The right to be informed about the collection and use of their personal data and the lawful basis for processing
- The right of access to information GRCC holds on them
- The right to rectification of inaccurate information held by GRCC
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

This applies to employed staff, volunteers, Trustees and service users, as well as applicants for roles at GRCC and other stakeholders.

GRCC has processes in place for individuals to follow, set out clearly within its Privacy Notice. GRCC also has internal processes in place to progress any subject request within the GDPR timescales.

## 14. Data Processors on behalf of GRCC

At point of contract, sign up to services or at data transfer, Data Processors for GRCC will be required to demonstrate compliance with GDPR.

## 15. Procedure for assisting the authority in responding to Freedom of Information requests

Statutory authorities and other public bodies are required to respond to requests under the Freedom of Information (FOI) Act 2000. In some cases GRCC may hold relevant information and be approached by the local authority for information. GRCC will require full details from the local authority about the nature of the request and the information required from GRCC, in order to make a decision about whether or not GRCC is willing to provide the information. Requests should be made by the local authority to the appropriate GRCC management lead within 5 days of receiving the request from the member of the public. This will provide GRCC with time to consider the request and to locate the relevant information as appropriate.

Decisons about whether or not to disclose will be made within 3 working days and the relevant information passed on (if appropriate) within 10 working days of the request being made to GRCC.

## 16. Review

This policy will be reviewed by GRCC Senior Leadership Team at least annually or when there are changes in legislation, to ensure it remains up to date and compliant with the law. The policy is subject to approval by the GRCC Board of Trustees.

## Declaration

I confirm I have read and understood GRCC's Data Protection and Information Governance Policy and will act in accordance with it.

I am connected with GRCC in my capacity as a

☐ Member of staff

☐ Volunteer

☐ Trustee

Signature:

Print name:

Date:

Please return this form to the Management Accountant unless you have completed a form covering a number of GRCC's policies.