

DATA HANDLING AND PROTECTION POLICY

Version	1.2
Document Status	LIVE
Document Owner	Compliance Officer
Last Reviewed	February 2025
Last Approved by	Governance Sub Group of the Board of Trustees
Next Review	January 2027
Applies to	All Trustees, Managers, Staff, and Volunteers who handle or have access to personal data as part of their role.

Data Handling and Protection Policy

1. Introduction

In our work at Space @ The Broomhouse Hub, we collect, process, and store personal data concerning our employees, volunteers, fundraisers and program participants. The UK's data protection legislation, including the General Data Protection Regulations (GDPR) contains strict principles and legal conditions which must be followed before and during any processing of any personal information.

It is every person's responsibility to comply with the principles and legal requirements of data protection legislation, including the GDPR and failure to meet those responsibilities are likely to lead to serious consequences.

The purpose of this policy is to ensure that everyone understands what personal data is, how it can be gathered and used. What processing means and how to make sure we always follow the law. For example, if an employee knowingly or recklessly discloses personal data in breach of the data protection legislation, including the GDPR, they may be held personally criminally accountable for any such breach. Also breach of the data protection legislation, including the GDPR rules, can cause distress to the individuals affected by the breach and is likely to leave the Company at risk of serious consequences.

If anyone is in any doubt about what they can or cannot disclose and to whom, they should not disclose the personal information until they have sought further advice from the Data Protection Representative (DPR).

It is mandatory that our trustees, all employees, volunteers, program participants and contractors read, understand and comply with the content of this policy and they must attend associated training relating to its content and operation.

2. Definitions

Personnel: In this document, the term 'personnel' refers to both employees and volunteers of Space @ The Broomhouse Hub.

Data Subject: Any living individual whose personal data is processed.

Data Controller: Space @ The Broomhouse Hub will be 'data controllers' in several ways, including:

- As an employer processing the personal data of employees, trustees and volunteers.
- As a provider of personalised services to beneficiaries and clients.
- As a fundraising or campaigning organisation that has donors and supporters.

Individual fundraisers may also be data controllers where they are acting independently of a charity in processing data.

Data Protection Legislation: This policy meets the requirements of the UK General Data Protection Regulation (UK-GDPR), the Data Protection Act (DPA) and the Privacy and Electronic Communications Regulations (PECR). In addition, guidance published by the Information Commissioners Office (ICO) has been considered.

Personal data: is any information that identifies a living individual (data subject) either directly or indirectly. This also includes special categories of personal data. 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.

Processing: is any activity relating to personal data which can include accessing, viewing collecting, recording, storing, editing, disclosing, transferring, retrieving, using or destruction.

Special categories of personal data: this includes any personal data which reveals a data subject's, ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.

Criminal records data: means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Breach: is a security incident in which the confidentiality, integrity, or availability of personal data is compromised. A data breach may include, but is not limited to, incidents such as:

- **Emails sent to incorrect recipients:** Sharing sensitive information about a beneficiary, donor, or employee with an unauthorised individual.
- **Misplaced physical documents:** Losing paper records that contain personal data, such as registration forms, health information, or contact details.
- **Unauthorised access to internal systems:** For example, a breach of IT security allowing third parties to access databases containing personal information.
- **Lost or stolen electronic devices:** If a device containing personal data, such as a laptop or USB drive, is lost or stolen without proper encryption.
- **Unauthorised disclosure of information:** Sharing personal details of beneficiaries or donors in public posts or on social media without explicit consent.

3. General provisions

- a. This policy applies to all personal data held on a filing system by Space @ The Broomhouse Hub, regardless of whether it is in paper or electronic format.

- b. This policy applies to all individuals whose personal data is processed by Space @ The Broomhouse Hub including:
 - Our trustees
 - Our staff, contractors, and volunteers
 - Local members
 - Our donors and fundraisers
 - Individuals using our services
 - Visitors to our website
- c. The Board of Trustees holds overall responsibility for data protection compliance within Space @ The Broomhouse Hub and will make key decisions regarding the processing of personal data. However, the Board of Trustees has appointed a dedicated individual to oversee data protection within our organisation. The Data Protection Representative (DPR) for the charity and is responsible for the day-to-day implementation of data protection policies and procedures. The DPR is the primary contact for the charity for any questions related to this policy or data protection matters.
- d. All staff, contractors and volunteers working on behalf of our charity have a responsibility to comply with this policy when processing personal data.
- e. This policy shall be reviewed periodically.
- f. The Charity shall register with the Information Commissioner's Office (ICO) as an organisation that processes personal data.

4. Roles and Responsibilities

The Board of trustees have a responsibility to:

- Follow the Scheme of Delegation, and where responsibility lies with the Board of Trustees, to ensure:
 - relevant skilled parties review policies at regular intervals to check for compliance with legislation and best practice
 - policies are implemented and utilised effectively

The Data Protection Representative (DPR) is responsible for:

- Being the primary contact for all data protection-related matters
- Managing and monitoring compliance with this Data Protection Policy and associated procedures.
- Providing guidance to personnel on data protection matters.
- Coordinating responses to data breaches, including notification to relevant authorities (e.g., the ICO) and affected data subjects, if necessary.
- Conducting periodic reviews of data processing activities to ensure ongoing compliance.

Line Managers have a responsibility to:

- Complying with Space @ The Broomhouse Hub's Data Protection Policy, relevant legislation, and procedures.
- Ensuring that this policy is accessible, understood, and followed by their teams.
- Acting promptly to report and address any data breaches or security incidents, including notifying the DPR.
- Leading investigations into data protection concerns in a fair and thorough manner.
- Maintaining consistency in managing their teams' adherence to data protection responsibilities.

Staff members and volunteers have a responsibility to:

- Comply with Space @ The Broomhouse Hub's Data Protection Policy, applicable laws, and their contracts or agreements.
- Prioritise the confidentiality, integrity, and security of personal data they process.
- Report any incidents, breaches, or suspected noncompliance to the DPR or their Line Manager immediately.
- Follow all procedures, including the use of privacy notices and obtaining consent, as applicable.

5. What are the GDPR principles?

Space is a data controller. This means that Space is required by law to ensure that all personnel who processes personal data and special categories of personal data during the course of their work with us does so in accordance with the data protection legislation, including the GDPR principles. In brief, the principles say that:

- a. Personal data must be processed in a lawful, fair and transparent way.
- b. The purpose for which the personal information is collected must be specific, explicit and legitimate.
- c. The collected personal data must be adequate and relevant to meet the identified purpose.
- d. The information must be accurate and kept up to date.
- e. 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.
- f. The personal data must be kept confidential and secure and only processed by authorised personnel.

Other rules under the GDPR state that:

The transfer of personal data to a country or organisation outside the UK/EEA should only take place if appropriate measures are in place to protect the security of that data.

The data subject must be permitted to exercise their rights in relation to their personal data.

The Company personnel must comply with these principles and rules at all times in their information-handling practices. Space is committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

Personnel must inform the Data Protection Representative immediately if they become aware that any of these principles or rules have been breached or are likely to be breached.

What are the lawful reasons under which Space would expect a Personnel to process personal data?

Whilst carrying out their activities, Space personnel are likely to process personal data. The Company will only expect personnel to process personal data where the business has a lawful basis (or bases) to process that information. The lawful basis may be any one of the following reasons or a combination of:

- a. Consent has been obtained from the data subject to process their personal data for specified purposes.
- b. Where we need to comply with a legal obligation.
- c. Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the data subject do not override those interests.

Space personnel must always ensure that they keep a documentary inventory of the legal basis (or bases) which is being relied on in respect of each processing activity which they perform.

Privacy Notices

Personal data must be processed in a lawful, fair and transparent way.

Before Space personnel begin collecting or processing personal data directly from a data subject, they must ensure that an appropriate privacy notice has been issued to the data subject. Different notices are used for employment and commercial purposes. The content of the privacy notice must provide accurate, transparent and unambiguous details of the lawful and fair reason for why we are processing the data. It must also explain how, when and for how long we propose to process the data subject's personal information. We need to include information around the data subjects' rights and most importantly, the notice should also explain how we will keep the information secure and protected against unauthorised use.

Where personnel intend to collect data indirectly from a third party or a public source (i.e. LinkedIn), they must ensure that a privacy notice is issued to the data subject within a reasonable of period of obtaining the personal data and no later than one month.

Personnel must only use data collected indirectly if they have evidence that it has been collected in accordance with the GDPR principles.

In all circumstances personnel must check that they are using an up-to-date version of the Company's privacy notice, and it is being used in accordance with the Company's guidelines.

Purpose Limitation

The purpose for which the personal information is collected must be specific, explicit and legitimate.

When Space personnel collect personal information, they will set out in the privacy notice how that information will be used. If it becomes necessary to use that information for a reason other than the reason previously identified, they must usually stop processing that information. However, in limited circumstances they can continue to process the information provided that their new reason for processing the personal information remains compatible with their original lawful purpose (unless their original lawful basis was consent).

Adequate and relevant

The collected personal data must be adequate and relevant to meet the identified purpose.

Space personnel must only process personal data where they have been authorised to do so because it relates to their work, or they have been delegated temporary responsibility to process the information. The personnel must not collect, store or use unnecessary personal data and they must ensure that personal data is deleted, erased or removed within the Company's retention guidelines. Personnel must not process or use personal data for non-work-related purposes.

The Company will review its records and in particular personnel files on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there are lawful reasons requiring information to continue to be held.

Accurate and kept up to date

The information must be accurate and kept up to date.

If a personnel private information changes, for example they change address or they get married and change their surname, they must inform their line manager as soon as practicable so that the Company's records can be updated. Space will not be responsible for any inaccurate personal data held on its systems where the person has failed to notify it of the relevant change in circumstances.

Kept for longer than is necessary.

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.

Different categories of personal data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed.

Kept confidential and secure

The personal data must be kept confidential and secure and only processed by authorised personnel.

To achieve this, personnel must follow these steps:

- Space @ The Broomhouse Hub has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data.
- Where Space provides code words or passwords to be used before releasing personal information, for example by telephone, they must strictly follow the Company's requirements in this regard.
- Only transmit personal information via email to external recipients if a secure network is in place. Internal communications are secure and do not require additional measures.
- Ensure that any personal data is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- Do not access another personnel record without authority as this will be treated as gross misconduct and it is also a criminal offence.
- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.
- Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable the employee to carry out their job duties and has been authorised by their line manager.
- Ensure that when working on personal information as part of their job duties when away from their workplace and with the authorisation of their line manager, they continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security.

- Ensure that hard copy personal information is disposed of securely, for example cross-shredded.
- Manual personnel files and data subject files are confidential and are stored in locked filing cabinets. Only authorised personnel have access to these files. For a list of authorised Personnel, please contact the Company's HR/DPR. These will not be removed from their normal place of storage without good reason.
- Data stored on memory sticks, discs, portable hard drives or other removable storage media is kept in locked filing cabinets.
- Data held on computers are stored confidentially by means of password protection.
- The Company has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed.

6. Transfer to another country

Transfer of personal data to countries or organisations outside of the UK/EEA should only take place if appropriate measures are in place to protect the security of that data.

We do not generally have a need to transfer data outside of the United Kingdom. However, if personnel are requested to transfer personal data to a country or organisation outside of the UK/EEA, Space @ The Broomhouse Hub ensures that any transfer of personal data complies with:

- Adequate Level of Protection:** We will only transfer personal data to a country or organisation outside the UK/EEA if that country or organisation provides an adequate level of data protection, as determined by the UK or EU authorities.
- Appropriate Safeguards:** If the destination country does not meet these adequacy standards, Space @ The Broomhouse Hub will implement additional safeguards to protect the data.
- Approval Process:** Any transfer of personal data outside the UK/EEA requires prior consultation and approval from the Operations Director or DPR to ensure that all necessary measures are in place to protect the data.

7. Closed Circuit TV (CCTV) Recording

Space @ The Broomhouse Hub collects video CCTV images of people entering and moving around its premises in order to safeguard its property from theft and vandalism, as required by its insurers. The information collected is only processed and, where appropriate, shared with other authorities (e.g. the Police) where it is necessary to investigate a potential crime.

8. The Data Subject Rights

The data subject must be permitted to exercise their rights in relation to their personal data.

Under the GDPR, subject to certain legal limitations, data subjects have available a number of legal rights regarding how their personal data is processed. At any time, a data subject can request that the Company should take any of the following actions, subject to certain legal limitations, with regard to their personal data:

- Allow access to the personal data.
- Request corrections to be made to data.
- Request erasure of data
- Object to the processing of data
- Request that processing restrictions be put in place.
- Request a transfer of personal data.
- Object to automated decision making.
- Right to be notified of a data security breach

There are different rules and timeframes that apply to each of these rights.

How should you respond to a data subject request?

Space personnel must follow the Company's data subject access procedure which details how to deal with requests, and it describes the circumstances where a fee may be charged. The procedure includes the following:

- Always verify the identity of the person making a data subject request and the legitimacy of the request.
- If you are unsure as to whether you are authorised to action the request, check the privacy notice to ascertain who is authorised to deal with data subject requests. If you are still unsure how to handle the enquiry, you should forward this to the Data Protection Representative.
- If you are authorised to deal with the request do not give out confidential personal information unless you have received the appropriate consent from the data subject. Seek explicit written consent to process the data subject request and ensure that they keep a clear audit trail of the request and their response.
- Do not share personal information with a third party, unless the data subject has given their explicit prior consent to the sharing of their information. A third party is anyone who is not the actual data subject and can include a family member of the data subject.
- Take great care not to accidentally share information with an unauthorised third party.
- Be aware that those seeking information sometimes use deception in order to gain access to it.

9. Categories of Information

During the course of their employment, personnel may be required to process personal data, which falls into different categories, general personal data and special categories of personal data. All data should be processed in accordance with the privacy notice and at all times in a confidential manner. However, where that data is classed as a special category extra care should be taken to ensure the privacy and security of that data. This means that they should maintain a high level of security and they should only share this data with those who are also authorised to process that data. In the context of employee relations, the scenarios when they may be required to process special categories information may arise for one or more of the following reasons:

- In order to comply with employment and other laws when processing and managing situations connected with absences arising in relation to sickness or family/ dependant related leave.
- To ensure health and safety obligations and other employment related obligations are met they may be required to process information about the physical or mental health or disability status of an employee in order to assess their capability to perform a role. The employee may also be required to monitor and manage sickness absence, recommend appropriate workplace adjustments and administer health related benefits.
- Where it is needed in the public interest, for example for equal opportunity monitoring and reporting.
- And any other reasons for which we inform the personnel under a separate policy or notice.

There may also be circumstances where we ask the personnel to process this type of information in relation to assisting the Company with legal claims or to protect a data subjects' interests (or someone else's).

Personnel may be asked to process information in relation to criminal convictions. Criminal Records Data, includes information obtained through PVG Membership. This data is processed solely for safeguarding purposes to assess the suitability of individuals working with vulnerable groups. Space @ The Broomhouse Hub is committed to ensuring that this data is handled in line with GDPR requirements, safeguarding principles, and organisational policies.

- Access to PVG Membership data is restricted to authorised personnel.
- PVG data is stored securely in electronic systems with access controls (SharePoint) or in locked physical storage.
- Data is retained only as long as necessary for safeguarding purposes and deleted securely thereafter.
- Logs of access are maintained to comply with GDPR and ensure transparency.
- Unauthorised access to PVG data is considered a breach of this policy and GDPR, subject to investigation and possible disciplinary action.

If the personnel is unsure about how they should process general personal data or special categories of personal data, they must contact the Data Protection Representative.

10. When Will Personnel Need to Seek Consent?

In limited circumstances during the personnel's work, they may need consent from a data subject in order to process personal data or special categories of data. They will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought.

However, in limited circumstances, the personnel may find it necessary to request a data subject to provide written consent to allow the processing of special categories of personal data. The employee will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought. For example, in an employment context the employee should request the data subject's written consent to instruct a medical practitioner to prepare a medical report. If it becomes necessary to request consent to process special categories of personal data, they must provide the data subject with details of the information that will be required and why it is needed, so that they can make an informed decision as to whether they wish to provide consent.

The employee must not compel a data subject to provide written consent. Giving consent will always be a decision made by freewill and choice and is not a contractual condition. Consent can be withdrawn at any time without any reason provided. The employee must not subject a data subject to a sanction or detriment as a consequence of withdrawing consent.

11. Exemptions

In limited circumstance there are certain categories of personal data which are exempt from the GDPR regime. In employment for example:

- Confidential references that are given, but not those received by the Company from third parties. Only CEO and HR can give Company references. Confidential references will not be provided unless the Company is sure this is the person's wish.
- Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
- Data which is required by law to be publicly available.
- Documents subject to legal professional privilege.
- In an emergency. You may share information with law enforcement or other emergency services such as Ambulance staff if the person is in danger, needs treatment or cannot respond themselves.

12. Action to be Taken in the Event of a Data Breach

A personal data breach will arise whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on a data subject.

In the event of a security incident or breach, Personnel should not try to handle this themselves.

They must immediately inform the Data Protection Representative so that steps can be taken to:

- Contain the breach.
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope of the breach by taking steps to contain and mitigate the breach.

The Data Protection Representative or a Senior Manager will determine within 72 hours the seriousness of the breach and if the Information Commissioner's Office (ICO) and/or data subjects need to be notified of the breach.

Please refer to the **Appendix 1** to follow the detailed guidelines for managing a breach.

For more information on handling a data breach and notification obligations, please refer to the official Information Commissioner's Office (ICO) [page](#).

13. Training

All Personnel that handle personal information of individuals must have a basic understanding of the data protection legislation, including the GDPR. Personnel with duties such as computer and internet security, marketing and database management may need specialist training to make them aware of particular data protection requirements in their work area.

Space will provide continuous training and updates on how to process personal data in a secure and confidential manner and in accordance with the spirit of the data protection legislation, including the GDPR. Personnel will be required to attend all training and to keep themselves informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.

Personnel must regularly review all their data processing activities and ensure that they are acting in accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

Annual refresher training will be mandatory, if applicable, to ensure ongoing compliance awareness.

14. Sharing Personal Data

Space share personal data internally as is necessary. Space personnel must always ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents. Extra care and security must be taken when sharing special categories of data or transferring data outside of the Company to a third party.

15. Direct Marketing

Space is subject to specific rules under the GDPR in relation to marketing our services. Data subjects have the right to reject direct marketing, and we must ensure that data subjects are given this option at first point of contact. When a data subject exercises their right to reject marketing, they must desist immediately from sending further communications.

16. Data Sharing with Partners

When sharing personal data with external partners, Space @ The Broomhouse Hub is committed to ensuring that such data sharing is performed securely and in compliance with data protection legislation. Before any data is shared with a partner, the following steps must be taken:

- a. **Data Sharing Agreement:** A formal Data Sharing Agreement (DSA) must be in place, outlining the purpose of the data sharing, the specific data to be shared, and the responsibilities of each party regarding data protection.
- b. **Purpose and Limitations:** Personal data should only be shared with partners for specific, legitimate purposes that align with Space @ The Broomhouse Hub's privacy policies and the original consent obtained from the data subjects. The shared data must not be used for purposes beyond those outlined in the Data Sharing Agreement.
- c. **Security Measures:** The partner organisation must demonstrate adequate security measures to protect the shared data from unauthorised access, loss, or misuse.
- d. **Regular Review:** Data-sharing agreements and practices should be reviewed periodically to ensure ongoing compliance with data protection laws and any changes in organisational needs or regulations.

Personnel must consult with the Data Protection Representative (DPR) before initiating any data-sharing activity to ensure these standards are upheld.

17. Data retention and destruction

Space @ The Broomhouse Hub is committed to retaining personal data only for as long as it is necessary to fulfil the purposes for which it was collected, in line with legal, operational, and financial requirements. Once the retention period expires, data will be securely deleted or destroyed.

Retention Periods for Different Categories of Data

- a. **Service Users:** Personal data of service users will be retained for 6 years after they cease using the service. This period is calculated from the date of their last interaction with the service.
- b. **Volunteers:** Volunteer information will be retained for 6 years after their involvement ends.
- c. **Young People:** Data for young people will be retained for 7 years after they cease using the service.
- d. **Young People on the Child Protection Register:** Information on young people listed on the Child Protection Register will be retained indefinitely.
- e. **Staff:** Staff records will be retained for 7 years after their employment ends, in line with employment law and taxation regulations.
- f. **Trustees:** Data relating to trustees will be retained for 6 years after their tenure ends.
- g. **Volunteers:** Volunteer records will be retained for 3 years after their last recorded activity.
- h. **Financial Records:** Financial records, including those containing personal data, will be retained for 6 years, in compliance with financial regulations.
- i. **Accidents:** Data related to accidents, including reports and investigations, will be retained for 5 years from the date of the incident, in accordance with health and safety regulations.
- j. **Complaints:** Records related to complaints, whether from employees or customers, will be retained for 5 years from the resolution of the case, to comply with potential legal claims and improve our service.

Data Disposal

When the retention period for any category of personal data expires:

- Data will be securely deleted (electronic records) or destroyed (physical records).
- Disposal methods will include secure shredding for paper records and data wiping for electronic records.

18. Complaints

If personnel believe that this policy has been breached by a colleague or to exercise all relevant rights, queries or complaints please in the first instance contact the Company's Data Protection Representative.

19. Changes to this Policy

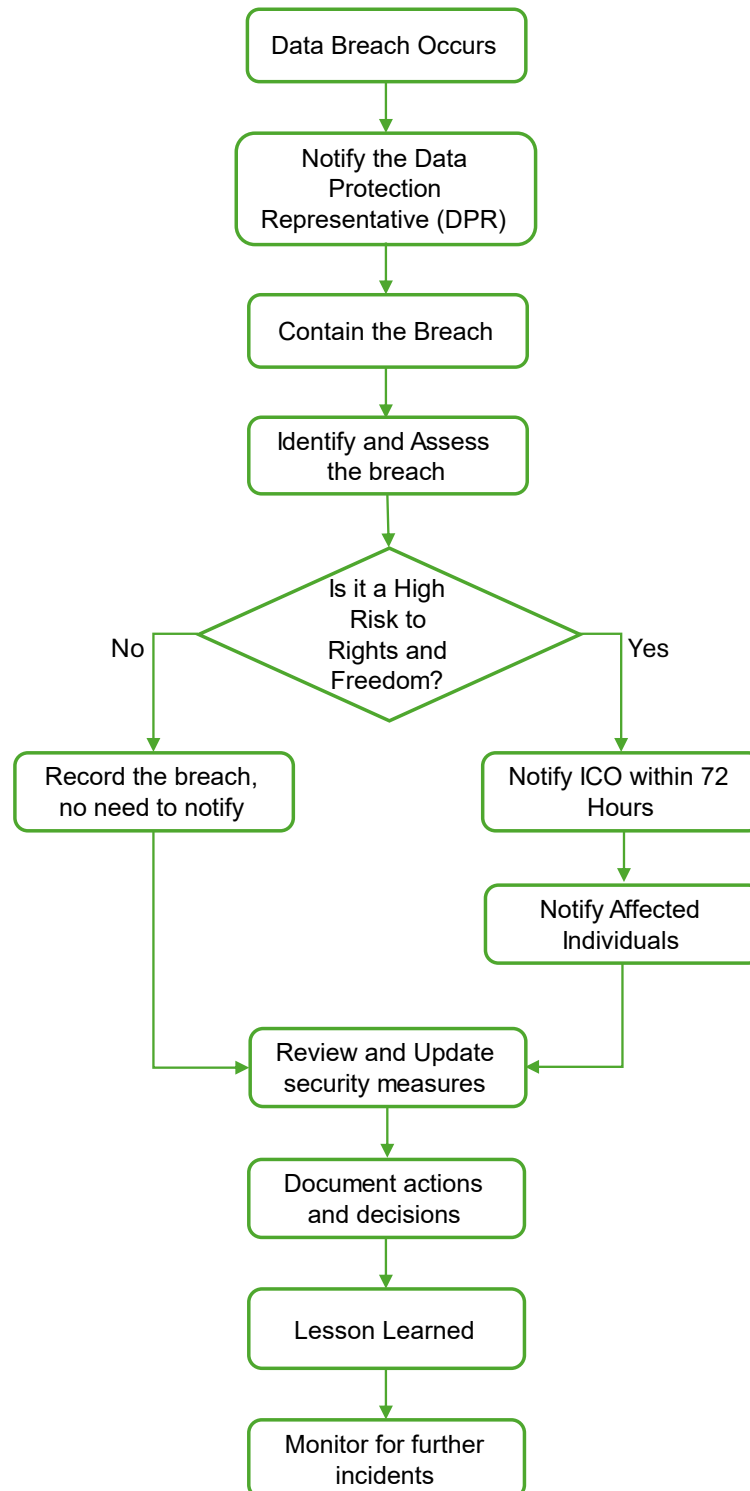
The Company reserves the right to make changes to this policy at any time so personnel should check this document regularly to ensure they are following the correct procedures.

20. Compliance With GDPR is Everyone's Responsibility.

Complying with this policy and GDPR and Data Protection regulations is every personnel responsibility. Having read this policy if the personnel does not understand what is expected of them and their responsibilities, they must speak to their line manager or the Data Protection Representative. All personnel have been asked to read this policy and adhere to the content. Any breach of any aspect of this policy may lead to serious disciplinary action.

Appendix 1

Actions to be taken in the event of a data breach



Step by Step

1. **Data Breach Occurs:** The process begins when a data breach is detected. This could include any unauthorised access, disclosure, or loss of personal data.
2. **Notify the Data Protection Representative (DPR):** As soon as the breach is identified, it's crucial to immediately inform the Data Protection Representative. This ensures that the organisation's designated person is aware of the incident and can coordinate the response.
3. **Contain the Breach:** The first priority after notifying the DPR is to take immediate action to contain the breach. This may involve stopping further data loss, securing systems, or restricting access to sensitive information to prevent additional exposure.
4. **Identify and Assess the Breach:** With the breach contained, the next step is to analyse and evaluate the incident. The DPR should work with relevant personnel to understand the scope of the breach, what data was affected, and how it may impact individuals.
5. **Risk to Rights and Freedom?** After assessment, determine if the breach poses a risk to individuals' rights and freedoms. This assessment will dictate the next steps in the response.
6. **If Yes:**
 - a. **Notify the ICO within 72 Hours:** If the breach poses a significant risk, notify the Information Commissioner's Office (ICO) within 72 hours of discovery.
 - b. **Notify Affected Individuals:** In addition to the ICO, inform the individuals whose data was compromised. Provide them with information on the breach and steps they can take to protect themselves.
7. **If No:**
 - a. **Record the Breach:** If the breach does not present a significant risk to individuals' rights and freedoms, document the incident in internal records. In this case, there is no need to notify the ICO or affected individuals.

8. **Review and Update Security Measures:** After managing the immediate breach, evaluate and improve security measures as necessary. This helps prevent similar incidents in the future and strengthens overall data protection practices.
9. **Document Actions and Decisions:** Thoroughly document each action taken and decision made during the breach response. This helps with compliance and can be valuable for future training and improvement.
10. **Monitor for Further Incidents:** Continue monitoring for any additional issues that may arise from the breach. Ongoing vigilance helps detect any delayed impacts and ensures that the organisation can respond quickly if related incidents occur.

Policy Version Control

Change made by	Date	Brief description of change	Version Number
Alexis Ciani	January 2025	Full policy review to ensure compliance with legislation and best practice	1.2