Data Protection Policy

Introduction

CRIN is committed to protecting the rights and privacy of individuals. In carrying out our day to day operations and meeting our legal obligations, we need to collect and use certain types of personal data.

CRIN is committed to compliance with the Data Protection Act 2018 and the EU General Data Protection Regulation 2016 and therefore regards the lawful and responsible handling of personal information as a fundamental obligation.

The aim of this policy is to ensure that everyone collecting or processing personal data is fully aware of the requirements of this legislation and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

EU General Data Protection Regulation

CRIN commits to full compliance with the EU General Data Protection Regulation.

The GDPR sets out seven principles key principles for the processing of personal data, which govern CRIN's approach to data protection:

1. **Lawfulness, fairness and transparency.** Personal data shall only be collected or processed for lawful grounds and never used in a way that is unduly detrimental, unexpected or misleading to the individual concerned.
2. **Purpose limitation**. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. **Data minimisation.** The collection and processing of personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
4. **Accuracy.** Personal data shall be accurate and, where relevant, kept up to date.
5. **Storage limitation**. Personal data shall not be kept for longer than is necessary for that purpose or those purposes.
6. **Integrity and confidentiality (security).** Appropriate security measures will be put in place to protect the personal data that is held.
7. **Accountability.** Appropriate measures will be taken and records made to demonstrate compliance with data protection principles and requirements.

For all personal data that CRIN holds or processes, there must be a legitimate ground for doing so:

1. **Consent.** A person has given us specific permission to hold and process their personal data.

2. **Contract.** Holding and processing the personal data is necessary for us to fulfil our contractual obligations or to enter into a contract.
3. **Legal obligation.** We are legally obliged to hold or process personal data.
4. Vital interests. The holding or processing of personal data is necessary for the life of a person.
5. **Public task.** The holding or processing of data is necessary to carry out an official authority or task set out in law.
6. **Legitimate interest.** We have another legitimate interest in holding or processing personal data, where there is a minimal privacy impact or a compelling justification for the processing.

CRIN commits to upholding the data rights of every person whose personal data we hold. Specifically:

1. Right to be informed.
2. Right to access.
3. Right to rectification.
4. Right to erasure.
5. Right to restrict processing.
6. Right to data portability.
7. Right to object.
8. Rights related to automated decision making, including profiling.

Individuals may exercise these rights by contacting CRIN verbally or in writing, but a staff member receiving such a request must keep a record of that request. For guidance in how to respond to such a request, see below.

Types of information processed

CRIN holds three types of information which are covered by this policy:

- Organisational information - publicly available information about organisations
- Personal information - information about individuals such as names, addresses, email addresses, phone numbers, job titles, passport information and bank details.
- Sensitive personal data - information about race, ethnic origin, politics, religion, trade union membership, health data.

Responsibilities

Overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of CRIN, this is the Council.

The governing body delegates tasks to the Data Controller. The Data Controller is responsible for:

The governing body delegates tasks to the Data Controller. The Data Controller is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures

All employees, contracted workers, trustees, interns and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy will result in disciplinary proceedings.

Policy implementation

To meet their responsibilities, staff, trustees, interns and volunteers will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised. These include:
    - The right to be informed that processing is being undertaken
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances; and
    - The right to correct, rectify, block or erase information which is regarded as wrong information.

CRIN will ensure that:

- Everyone managing and handling personal information is trained to do so;
- Anyone wanting to make enquiries about the handling of personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data is in line with CRIN's procedures;
- Queries about handling of personal information are dealt with swiftly and politely.

Training

Training and awareness raising about the Data Protection Act and how it is followed within CRIN will take the following forms:

- On induction, staff and volunteers will be provided with CRIN's data protection policy and provided with guidance on how to address any data processing that may arise through their work.
- Ongoing training and awareness raising will be provided to staff and volunteers.

Subject access requests

Anyone whose personal information we process has the following rights to:

- Be informed of how their information is processed;
- Rectify inaccurate or incomplete information;
- Erase their personal information;
- Restrict the processing of their information;
- Data portability;
- Object to the processing of their data.

Individuals may exercise these rights by contacting CRIN verbally or in writing, but a staff member receiving such a request must keep a record of the request.

The following information will be required before access is granted:

- Full name and contact details of the person making the request;
- Their relationship with the organisation;
- The type of identification required before releasing any information;
- Any other relevant information.

Queries about handling personal information will be dealt with politely, without undue delay and in any event within one month. CRIN reserves the right to charge a reasonable fee to cover administrative costs in complying with a subject access request where the request is manifestly unfounded, excessive or where the individual requests further copies of their data following a request. Where staff require support or guidance in responding to a request, they should contact the Legal and Policy Director.

Destroying personal data

Personal data should only be retained for as long as it is needed and should be securely disposed of once it is not. CRIN will ensure that this information is securely destroyed at the end of the relevant retention period.

The following specific periods shall apply:

- Applications for jobs within CRIN will be retained for six months
- Personnel files and training records, including disciplinary records, will usually be retained for 6 years after employment ceases. However, the record shall be retained until at least retirement age, or for 10 years if that is longer, in any situation in which:
    - ❖ There were concerns about the behaviour of an adult who was working with children where they behaved in a way that has harmed, or may have harmed, a child;
    - ❖ The adult may have committed a criminal offence against, or related to, a child;
    - ❖ The adult behaved towards a child in a way that indicates that they are unsuitable to work with children.

Review

This policy will be updated as necessary to reflect best practice in data management and control and to ensure compliance with any changes or amendments made to relevant law.

This policy will be reviewed annually to ensure that it remains up to date and compliant with the law.

In case of any queries or questions in relation to this policy, please contact the Finance Officer.

Data security

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

- Password protection for personal information files;
- Back up of data on computers (onto a separate hard drive);
- All portable devices (including laptops, hard drives and USB sticks) to be encrypted; and
- Password protected attachments for sensitive personal information sent by email.

Anyone who makes an unauthorised disclosure of personal data to a third party will be subject to disciplinary proceedings.

The Board and trustees are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach that they have made.

Any unauthorised disclosure made by an intern or volunteer may result in the termination of their agreement.