GDPR policy

The GDPR policy outlines the way The Harry Garratt Foundation will handle data safely. The trustees will familiarize themselves with the information below and ensure good practice when handling data. Data shall be stored for the times required by the Charity Commission, HMRC etc and then will be removed from all storage completely.

This policy covers:

Personal Data

Such as

- name, date of birth and address

Sensitive or Special Category Data

Such as:

- Sexual orientation, gender realignment, ethnicity, physical and mental health
- Social care records, child protection or housing assessments
- Political opinions or trade union membership
- Religious beliefs
- DNA or fingerprints
- Financial or credit card details
- National Insurance number or tax, benefit or pension records
- Travel details, for example at immigration control, or Oyster records
- Passport number / information on immigration status
- Work record or place of work, school attendance or records
- Conviction, prison or court records

Corporate Data

Such as

- Contracts
- Minutes of meeting from business/corporate meetings
- Finance details.

.

GDPR policy

Freedom of Information Act

Under the Freedom of Information (FOI) Act 2000, public authorities have a legal obligation to provide information through an approved publication scheme and in response to requests. This act does not apply to personal information.

The FOI Act gives the public the right to request any information held by any type of public authority or by persons/organisations providing services for them. This includes educational institutions, NHS Trusts and contractors, local authorities etc.

The public can request information held within documents such as: minutes of meetings, work emails, work diaries, corporate reports and other work documents. Exemptions may apply for certain information, which therefore would not be disclosed.

Requests made to an organisation must be in writing and the person does not need to quote the FOI Act in the request. Organisations must respond in writing within 20 days.

Confidential Information

All clients have a fundamental right to confidentiality.

Sometimes it can be confusing to know what information is appropriate to share when dealing with other departments or agencies.

The guiding principles for GDPR outlined in the Caldicott report can be used to ensure best practice and are laid out below: The Trustees use the term client to cover all adults and children that interact with The Harry Garratt Foundation

Principle One - "Justify the purpose"

Every proposed use or transfer of client identifiable information within or from an organisation, should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian

Principle Two - "Don't use client -identifiable information unless it is absolutely necessary"

Client-identifiable information items should only be used when there is no alternative.

Principle Three - "Use the minimum necessary client-identifiable information"

Where use of client-identifiable information is considered to be essential, each individual item of information should be justified with the aim of minimising personal data transferred.

Principle Four - "Access to client- identifiable information should be on a strict need-to-know basis"

Only those individuals who need access to client-identifiable information, should have access to it, and they should only have access to the information items that they need to see.

GDPR policy

Principle Five - "Everyone should be aware of their responsibilities"

Actions should be taken to ensure that those handling client -identifiable information are aware of their responsibilities and obligations to respect client confidentiality.

Principle Six - "Understand and comply with the law"

The use of client-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with the legal requirements.

Principle 6 -Information Sharing

"The duty to share information can be as important as the duty to protect client *confidentiality".*

Handling Data Breaches

As the use and variety of data has increased, the importance of collection, storage and transfer of data has led to the introduction of GDPR and the Data Protection Act 2018. These include strict rules to report data breaches to ensure that data can be secured as effectively as possible and lessons are learnt.

A data breach, accidental or deliberate can include destruction, loss, alteration or unlawful access to personal data. It is important to understand that this can be both physical and digital data - maybe a ransomware attack on a network system or losing a paper-based file which includes patient data.

Upon discovering a data breach, you should follow your organisation's reporting policy and ensure your Data Protection Officer (DPO) or Data Protection Champion (DPC) are made aware immediately and can assist and respond to the breach within 72 hours, as may be required by the Data Protection Act.

Collecting Data

Data related to an individual can be expressed as either **Personal Data** or within a sub-category of Personal Data called **Sensitive Data or Special Category Data.**

Personal Data

If a person, referred to as a data subject, can be identified directly or indirectly by information held, this is considered personal data. This can include;

- Name, Date of Birth, National Insurance number and contact information
- HR records, medical records or convictions
- Personal opinions of an individual's work performance or job application

Sensitive Data or Special Category Data

A person's religious or ethnic origin, religious beliefs or political opinion would be regarded as Sensitive Data. This information is often not required to be gathered by an organisation. If an organisation does not require to be collected it should be considered to not request it.

GDPR policy

In all cases, prior written consent from the data subject needs to be given before any personal or sensitive data is requested, and data should only be kept as long as necessary.

Storage

Ask yourself:

- Are the paper files stored safely in lockable cabinets or secure areas?
- Is the electronic data securely stored, e.g. encrypted or password-protected?
- Do you ever upload personal information to external websites such as Dropbox?
- Is data stored only for a specified time, or is it kept longer than is strictly necessary?
- Do you securely dispose of data?

Access

Ask yourself:

Is your computer screen clearly visible to passers-by?

- Is there a 'clear desk' policy - not leaving files or papers lying around - and do you follow it?
- Is it necessary for you to take personal data off-site - either to meet clients, or when working at home? If so, how secure is it?
- Are your computer, laptop or portable storage devices password-protected?
- Is the Wi-Fi access secure?
- Do you share passwords with colleagues?
- Are you and your colleagues logged on to each other's computers?

Sharing

Ask yourself:

- Is confidential post correctly addressed and marked as confidential?
- Are confidential emails encrypted and secure?
- Do you always clearly state that the information is confidential?
- Do you check caller identities before revealing personal information over the phone?
- Do you ever leave confidential information on a voicemail?
- Do you ever discuss confidential information in a public setting, e.g. an open office or cafe?
- Is confidential information only discussed with those who strictly need to know?

GDPR policy

Your Responsibility

It is your responsibility to keep all personal and sensitive information secure.

Protecting information and remaining vigilant will reduce the risk of a breach.

This can be done by protecting your passwords, transferring information securely and reporting security breaches to your Data Protection Officer and line manager.

More information can be found below.

Human Rights Act 1998

The Human Rights Act | Equality and Human Rights Commission (equalityhumanrights.com)

The Data Protection Act 2018

Data Protection Act 2018 - GOV.UK (www.gov.uk)

General Data Protection Regulation (GDPR)

November 2024 – update November 2025