



## GDPR and Data Protection Policy

### Policy Statement

Kehelland Trust is committed to preserving the confidentiality, integrity and availability of all of the physical and electronic data which it collects, stores

and uses.

### Policy Aim

The aim of this policy and associated procedures is to ensure that any personal data is kept securely and is properly protected from unlawful or unauthorised processing, loss, destruction or damage in line with the legal requirements set out in UK GDPR and the Data Protection Act 2018 enforced by the Information Commissioner's Office (ICO).

### Introduction

Kehelland Trust needs to ensure that its data collection, use, retention and security is UK GDPR compliant. This policy will outline accountability and internal procedures to ensure compliance with Article 5 of the UK GDPR which requires that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals.
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- d) 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.
- e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) 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."

### Policy Application

The following people may be affected by this policy:

1. All staff and volunteers
2. All trainees and learner
3. Customers
4. Family members/ carers/ advocates
5. External partners/ health professionals
6. The Local Authority and other funders.

### Definitions:

"Processing" is defined as any operation or operations performed on personal data, such as collection, recording, structuring, storing, alteration, retrieval, disclosure, combination, restriction erasure or destruction.

"Personal data" is defined as any information held about a living, identifiable individual. Individual identification can be by information alone or in conjunction with other information.

"Special category data" requires additional protection and is defined in UK GDPR as data about:

- Health
- Racial or ethnic origin

“Special category data” requires additional protection and is defined in UK GDPR as data about:

- Health
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where processed to identify a person)
- Sex life or sexual orientation.

The processing of criminal offence data also has additional legal safeguards under DPA. Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions. This policy applies to personal, special category and criminal offences data held by the Trust as defined in the UK GDPR and DPA 2018. Anyone who processes personal, special categories of personal information or criminal offences data for the Trust must adhere to this policy.

## **Procedures**

### **1. The nomination of a Responsible Person**

The Board of Trustees met on 15<sup>th</sup> May 2018 and voted that the Responsible Person accountable to ensure that the Trust meets its obligations under the new regulations is Anthea Hedge.

### **2. Data Collection and processing**

By nature of the service that the Trust provides we need to collect sensitive and personal information to enable us to provide safe and effective care services/ support and education.

We will strive to ensure transparency of the information we collect, to this end we have developed:

- Privacy Statements which clearly specifies what data we collect, why we need this information, how we use it, how we store it and when we may need to share it.
- Consent forms to be read and signed by those whose data we need to collect, with the right to withhold/ withdraw consent at any time.

### **3. Data Security**

In order to ensure data security, the following procedures are in place:

- Any written data is stored in lockable, fire-retardant filing cabinets which are accessed by keys kept in the safe.
- Any digital data is stored on computers which are allocated to individuals within the organisation and are password protected. People unauthorised by Kehelland Trust to use these computers, such as partners or children, must not be allowed access to Trust devices.
- Access to our databases such as You Manage, Share Point, Dropbox and CPOMS is given dependent on role and level of responsibility. Remotely stored database information is kept in secure data centres located in the UK.
- Staff updates and training are in place to ensure understanding of the new regulations and how it impacts on them and the people we support.
- Consent is obtained from individuals before sharing data with any third party unless in the case of a medical emergency where information will need to be shared with medical professionals/ family/ carers.
- Kehelland Trust has purchased tablets and a camera for the purpose of taking photos of our service users. These tablets are kept in the safe which is fireproof and lockable.
- The main building which contains the filing cabinets is locked and alarmed overnight.
- Documents containing personal data to be shared by email are
  - password protected; the password can only be obtained by the recipient by telephoning the sender.
  - Sent securely using Egress Switch.

sender.  
➤ Sent securely using Egress Switch.

- Specialist IT support is employed by Kehelland Trust, with the ability to remotely access staff computers on request. This includes the ability to remotely delete data should the asset become stolen.

#### 4. Data Retention

As a general principle Kehelland Trust will not keep (or otherwise process) any personal data for longer than is deemed necessary in keeping with requirements by statutory organisations and/ or funders.

Staff records will be kept for 10 years due to pension requirements, service user records will be kept for 6 years after the person leaves.

#### 5. Subject Access Requests (SARs)

Requests for access to information must be made in writing to the CEO. We will endeavour to give you a copy of the data as soon as possible, but in any event within 1 month.

In certain circumstances, for example particularly complex or multiple requests, it can take a further 2 months to provide data. In this case, we will tell you:

- within 1 month of your request
- why there's a delay.

There are some situations when we are allowed to withhold information, for example, if the information is about:

- the prevention, detection or investigation of a crime.
- National security or the armed forces.
- The assessment or collection of tax.
- Judicial or ministerial appointments.

We do not have to say why we are withholding information if it falls into these categories.

We may also refuse to comply with a SAR if it is:

- manifestly unfounded; or
- manifestly excessive.

What does manifestly unfounded mean?

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right of access. For example, an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass the organisation with no real purpose other than to cause disruption. For example, the individual:
  - explicitly states, in the request itself or in other communications, that they intend to cause disruption.
  - makes unsubstantiated accusations against the Trust or specific employees which are clearly prompted by malice.
  - targets a particular employee against whom they have some personal grudge; or
  - systematically sends different requests as part of a campaign, eg once a week, with the intention of causing disruption.

Consideration must be given to the context in which it is made. If the individual genuinely wants to exercise their rights, it is unlikely that the request is manifestly unfounded.

Whilst aggressive or abusive language is not acceptable, the use of such language does not necessarily make a request manifestly unfounded.

What does manifestly excessive mean?

necessarily make a request manifestly unfounded.

What does manifestly excessive mean?

To determine whether a request is manifestly excessive we would need to consider whether it is clearly or obviously unreasonable. This is based on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request.

This will mean taking into account all the circumstances of the request, including:

- the nature of the requested information.
- the context of the request, and the relationship between the Trust and the individual.
- whether a refusal to provide the information or even acknowledge if we hold it may cause substantive damage to the individual.
- our available resources.
- whether the request largely repeats previous requests, and a reasonable interval hasn't elapsed; or
- whether it overlaps with other requests (although if it relates to a completely separate set of information, it is unlikely to be excessive).

A request is not necessarily excessive just because the individual requests a large amount of information. As stated above, we must consider all the circumstances of the request. We should also consider asking the individual for more information to help you locate the information they want and whether you can make reasonable searches for the information. Please see '[Can we clarify the request?](#)' and '[What efforts should we make to find information?](#)'.

Personal data can relate to more than one person. Therefore, responding to a SAR may involve providing information that relates to both the requester and another individual.

There is an exemption in the DPA 2018 that says we do not have to comply with a SAR, if doing so means disclosing information which identifies another individual, except where:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

For further detailed information about refusing a SAR, please refer to the ICO here:

[When can we refuse to comply with a request? | ICO](#)

### **What should we do if we refuse to comply with a request?**

If we need to refuse to comply with a request, we must inform the individual of:

- the reasons why.
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through the courts.

If we believe a request is manifestly unfounded or excessive, we must be able to demonstrate this to the individual. Where an exemption applies, the reasons we give to an individual for not complying with a request may depend upon the particular case. For example, if telling an individual that you have applied a particular exemption would prejudice the purpose of that exemption, our response may be more general. However, where possible, we should ensure that we are transparent about our reasons for withholding information.

## **6. Destroying Personal Data**

Kehelland Trust will implement processes for effectively destroying and/ or deleting personal data at the end of the relevant retention period. Hard copies of documents will be shredded, documents stored on computers will be deleted. Any piece of equipment used to store personal data that needs to be replaced will be destroyed by Focus Technology Europe Ltd, a certified WEEE contractor who have the expertise with which to ensure that this is done according to relevant legislation.

## **7. How you can update your information**

The accuracy of your information is important to us. For service users/ parents/ carers/ customers: If you change your address or email address, if any of your circumstances change or any of the

## 7. How you can update your information

The accuracy of your information is important to us. For service users/ parents/ carers/ customers: If you change your address or email address, if any of your circumstances change or any of the other information we hold is out of date, please inform the manager of the department that you are receiving services from.

Members of staff and volunteers please notify the HR Coordinator.

## 8. The rights of data holders

The GDPR provides the following rights for individuals:

1. The right to be informed of how we process your data.
2. The right of access to the data we hold about you.
3. The right to rectification (to have it amended if it is incorrect).
4. The right to erasure (for it to be deleted if we do not have a legal requirement to retain it).
5. The right to restrict processing.
6. The right to data portability.
7. The right to object to us using it.
8. The right to withdraw your consent if you no longer wish us to process (if applicable).
9. Rights in relation to automated decision making and profiling.

These rights are outlined within the Trust's **Privacy Notice** to ensure transparency.

## 9. Safeguarding

The police, safeguarding partners and Local Safeguarding Children Boards can require a person or an organisation to comply with a request for information. This can only take place when the information requested is for the purpose of enabling or assisting the safeguarding partners or LSCB to perform their functions. Any request for information to a person or body, will be necessary and proportionate to the reason for the request.

## 10. Data Breaches

Kehelland Trust understands that it may need to report data breaches to the ICO and to affected data subjects as well as commissioners such as the Local Authority. The Trust will also strive to ensure that potential data protection and security issues are identified and addressed as early as possible. Should it be necessary in the future, Kehelland Trust will conduct Privacy Impact Assessments to identify and reduce the privacy and security risks of any project, contract or processing carried out by the Trust.

## 11. Related Kehelland Trust Policies and Procedures

- Safeguarding Adults Policy
- Safeguarding Children Policy
- Whistleblowing Policy
- Anti-harassment and Bullying Policy
- Confidentiality Policy.

## 12. Review, Analysis and Feedback

The Trust will ensure that all staff and Trustees are involved in the process of review, evaluation and planning for improvements based upon these reviews and that any identified specific areas for improvement are documented, allocated and acted upon.

## 12. Complaints

If you have concerns regarding the way we have processed your information, please contact the CEO: Kehelland Trust, Kehelland, Camborne TR14 0DD, 01209 613153.

We would prefer any complaints to be made to us initially so that we have the opportunity to see if we can put things right. However, if you are unhappy with the way we have processed your information or how we have responded to your request to exercise any of your rights in relation to your data, you can raise your concerns directly with the Information Commissioners Office:

Telephone: 0303 123 1113

Website: <https://ico.org.uk/concerns/>

Breaches of this policy may result in disciplinary action being taken.

Kehelland Trust GDPR and Data Protection Policy

March 2025

for review March 2026