The Kennedy Trust for Rheumatology Research

Data Protection Policy

Version Control

Date adopted:	October 2014	**Review period:**	2 years
Date of last review:	August 2023	**Owner:**	General Purposes Committee
Date of next review:	August 2025	**Version:**	4

The Kennedy Trust for Rheumatology Research

Data Protection Policy

1. Introduction

The Kennedy Trust for Rheumatology Research (the "**Trust**") is committed to complying with its data protection obligations, and to being concise, clear and transparent about how it obtains and uses personal information relating to its workforce and other individuals, and how (and when) it deletes that information once it is no longer required.

This policy sets out how we comply with our data protection obligations set out in Retained Regulation (EU) 2016/679 (the "**UK GDPR**") and the Data Protection Act ("**DPA**") 2018, and seek to protect the personal data of our staff, Trustees, Committee members, researchers and other third parties who may come into contact with the Trust.

The aim of this policy is to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their work.

The Trust has appointed the Programme Manager for Research and Policy as the person with overall responsibility for data protection compliance within the organisation (the Data Protection Lead ("**DPL**")). Any questions about this policy or requests for further information should be directed to them at enquiries@kennedytrust.org.

2. Scope

This policy applies to all staff including employees, Trustees and Committee members.

Staff should refer to the Trust's Privacy Notices and, where appropriate, to other relevant policies including those relating to information security and data retention, which contain further information regarding the protection of personal data in those contexts.

We will review and update this policy on a biennial basis in accordance with our data protection obligations. This policy does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

All staff are required to read and confirm that they understand this policy.

3. Definitions

This policy uses the following definitions:

Term	Meaning
Criminal offence data	means all personal data relating to criminal convictions and offences or related security measures (including information about criminal activity, allegations or suspicions, investigations and proceedings);
Data subject	means an individual to whom personal data relates,
Personal data	means any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other available information;
Personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed;
Processed / Processing	means any actions performed on personal data, including collecting, recording, organising, structuring, storing, modifying, consulting, using, publishing, combining, erasing, and destroying data.
Special category personal data	means personal data afforded special protection by the UK GDPR. This includes information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation;
Information Commissioner's Office (ICO)	Means the UK's independent data protection and information regulator.

4. Data protection principles

When processing personal data, the Trust and its staff must comply with the data protection principles that are set out in Article 5 of the UK GDPR as follows:

- we will process personal information lawfully, fairly and in a transparent manner ('***lawfulness, fairness and transparency***');
- we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes ('***purpose limitation***');
- we will only process the personal information that is adequate, relevant and necessary for the specified purposes ('***data minimisation***');
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal data is deleted or corrected without delay ('***accuracy***');

- we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed ('***storage limitation***'); and
- we will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage ('***integrity and confidentiality***').

In addition, the Trust is also responsible for, and must be able to demonstrate compliance with the above principles ('***accountability***'). This means that the Trust will:

- inform individuals about how and why we process their personal data, usually by way of a privacy notice;
- be responsible for checking the quality and accuracy of the information;
- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with our Workforce Privacy Notice;
- ensure that when information is authorised for disposal it is disposed of or deleted appropriately;
- ensure appropriate security measures to safeguard personal information whether it is held in paper files or electronically;
- share personal information with others only when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access requests and other rights exercised by individuals in accordance with the UK GDPR;
- report any actual or suspected personal data breaches.

5. Lawfulness, fairness and transparency

The Trust is responsible for ensuring that personal data is processed in a lawful, fair and transparent way. In relation to any processing activity we will, before the processing begins, and then regularly while it continues:

- review the purposes of the particular processing activity, and identify which of the following legal bases for processing (as set out in Article 6 of the UK GDPR) is most appropriate:

  (i) that the data subject has ***consented*** to the processing;
  (ii) that the processing is necessary for the ***performance of a contract*** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
  (iii) that the processing is necessary for ***compliance with a legal obligation*** to which the Trust is subject;
  (iv) that the processing is necessary for the ***protection of the vital interests*** of the data subject or another natural person;

(v) that the processing is necessary for the purposes of legitimate interests of the Trust or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
- where special category personal data or criminal offence data is processed, also identify a lawful condition (as set out in Articles 9 and 10 of the UK GDPR, and Schedule 1 of the DPA 2018) for processing this type of information, and document it.

When determining whether the legal basis of legitimate interests is appropriate, we will:

- carry out a legitimate interests assessment ("**LIA**") (a type of light-touch risk assessment) and keep a record of it, to ensure that we can justify our decision;
- if the LIA identifies a significant risk to an individual's data protection rights, consider whether we also need to conduct a data protection impact assessment (see section 6);
- keep the LIA under review, and repeat it if circumstances change; and
- include information about our legitimate interests in our relevant privacy notice(s).

In the rare circumstances where processing of personal data is likely to result in a high risk to individuals, we will, before commencing the processing, carry out a data protection impact assessment ("**DPIA**") to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

In order to comply with its transparency obligations, the Trust will issue privacy notices from time to time, informing data subjects about the personal data that we collect and hold, how they can expect personal data to be used and for what purposes. We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

6. Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with the purpose(s) identified.

You must not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and they have consented where necessary.

7. Data minimisation

The Trust will ensure that it only processes the personal information that is adequate, relevant and necessary in relation to the purposes for which it is processed.

You may only collect personal data to the extent required for your duties, and should ensure that any personal data collected is adequate and relevant for the intended purposes. In order to do this, you should:

- minimise the processing of personal data, for example, through redaction and the deletion of long emails trails;
- anonymise personal data where appropriate;
- pseudonymise personal data where possible, for example, through the use of initials rather than full names; and
- ensure that when personal data is no longer needed, it is deleted in accordance with the Workforce Privacy Notice.

8. Accuracy

Personal data must be accurate and kept up to date. It must be corrected or deleted without delay when it is inaccurate.

Staff are responsible for helping the Trust keep their personal data up to date. You should let the DPL know if the information you have provided to the Trust changes, for example if you move house or change details of the bank or building society account to which you are paid.

9. Storage limitation

Personal data should not be kept in an identifiable form for any longer than is necessary for the purposes for which the personal data is processed, except where there is clear historic or research value to the retention of the information.

The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.

Personal information that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

10. Integrity and confidentiality

The Trust will use appropriate technical and organisational measures in accordance with our Workforce Privacy Notice to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the DPL.

All staff have an obligation to report actual or suspected personal data breaches to the DPL immediately upon discovery. Having been advised of an actual or suspected personal data breach, the DPL will inform the Trust's IT consultants who will enact their standard data breach protocol. This includes the following steps:

1. Blocking the account and resetting its password
2. Revoking any current online sessions
3. Checking for any evidence of the malicious actor trying to cover their intrusion (redirecting emails for example)
4. Looking for any backdoors created into the account
5. Reviewing the access logs to look for suspicious logons or locations
6. Performing a message/content trace to see if the account was used to distribute any emails

Only once the above steps have been satisfied will the user be assisted with logging back into their account. If necessary, the Trust's IT consultants will assist with establishing and remediating the attack vector, such as password re-use across sites and not using multi-factor authentication.

11. Documentation and records

We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve special category data or criminal offence data, including:

- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- where relevant, details of transfers of personal data outside the UK, including documentation of the transfer mechanism safeguards in place;
- where possible, retention schedules; and
- where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal information;
- DPIAs; and
- records of personal data breaches.

If we process special category data or criminal offence data, we will keep written records of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- the lawful basis and additional conditions relied upon to process this information; and
- whether we retain or erase the personal information and why.

We will conduct regular reviews of the personal information we process and update our documentation accordingly.

12. Individual obligations

You may have access to the personal information of other members of staff, Trustees Committee members, researchers and other third parties who may come into contact with the Trust in the course of your employment, Trusteeship or Committee membership. If so, the Trust expects you to help meet its data protection obligations to those individuals.

If you have access to personal data, you must:

- only access the personal data that you have authority to access, and only for authorised purposes;
- only allow other staff to access personal data if they have appropriate authorisation;
- only allow individuals who are not staff to access personal data if you have specific authority to do so from the DPL;
- keep personal data secure.

13. International transfers

The Trust will not transfer personal data outside the UK other than where necessary for the review and assessment of research funding proposals.

14. Training

The Trust will ensure that all staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, who are responsible for implementing this policy, or responding to information requests, will receive additional training to help them understand their duties and how to comply with them.

15. Consequences of failing to comply

The Trust takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed; and
- carries the risk of significant sanctions for the individual and the Trust; and

- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy any failure to comply with any requirement of it may lead to disciplinary action, which may result in termination of your relationship with the Trust.

16. Contact

If anyone has any concerns or questions in relation to this policy they should contact the DPL via enquiries@kennedytrust.org in the first instance.