**The Knapp Foundation**
Charity Registration Number 1200294

# Data Protection Policy

## Contents

## Aims

1. The Knapp Foundation aims to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether they be an employee, Trustee, visitor, contractor, consultant, or any other individual, is done so in accordance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018). This policy applies to all personal data processed by the Foundation, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in, and whether the collection or processing of data was, or is, in any way automated. It is subject to review every three years or to reflect changes in legislation or in the light of experience.

## Legislation and guidance

2. This policy meets the current requirements of UK Data Protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the EU GDPR, UK GDPR and DPA 2018. It is also based on the information provided by the Article 29 Working Party. Additionally, it meets the requirements of the Protection of Freedoms Act 2012, the ICO's code of practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information.

## Definitions

| Term | Definition |
|---|---|
| **Data controller** | The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| **Data processor** | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, following the Controller's instruction. |
| **Data subject** | The identified or identifiable individual whose personal data is held or processed. |
| **Consent** | Freely given, specific, informed and unambiguous indication of the data subject's wishes via a statement or by a clear affirmative action, signifying agreement to a specific processing of personal data relating to them. |
| **Personal data** | Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:<br>• a name,<br>• an identification number, |

- location data,
- an online identifier or
- to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Special categories of personal data**

Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Genetics,
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes,
- Health – physical or mental,
- Sex life or sexual orientation,
- History of offences, convictions or cautions *****

***** Note: While criminal offences are not listed as special category data, within this policy they are regarded as such in acknowledgment of the extra care which is needed with such data.

**Processing**

Any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing can be automated or manual.

**Data breach**

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

## The data controller

3. The Foundation collects and determines the processing of personal data relating to an employee, Trustee, visitor, contractor, consultant, or any other individual. In addition the Foundation processes data on behalf of others, and therefore is both a data controller and a data processor. The Foundation is registered as a data controller with the ICO and will renew this registration as legally required. The registration number is ZB391497.

.

## Roles and responsibilities

4. This policy applies to all individuals employed by the Foundation, and to external organisations or individuals working on our behalf. Employees who do not comply with this policy may face disciplinary action. The Trustees have overall responsibility for ensuring that the Foundation complies with all relevant data protection obligations.

5. The Foundation has appointed Prof. Laurence Hemming as its Data Protection Officer (DPO). Prof. Laurence Hemming is responsible for overseeing the implementation of this policy, along with any future development of this or related policies/guidelines, and for reviewing the Foundation's compliance with data protection law. Upon request the DPO can provide an annual report of the Foundation's compliance status directly to the Trustees and will report to the Trustees with his/her advice and recommendations on Foundation data protection issues. The DPO is also a named point of contact for all Data Subjects whose data the Foundation processes, and for the ICO.

6. Employees (regardless of role) are responsible for:

1) Collecting, storing and processing any personal data in accordance with this policy
2) Informing the Foundation of any changes to their personal data, e.g., a change of address, telephone number, or bank details.
3) Reporting a Data Breach, Data Right Request, or Freedom of Information Request.
4) Contacting the Data Protection Lead or DPO:
    a) With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    b) If they have any concerns that this policy is not being followed
    c) If they are unsure whether or not they have a lawful basis to use personal data in a particular way
5) If they need to rely on or capture consent, draft a privacy notice/notification, or transfer personal data outside the United Kingdom.
6) Whenever they are engaging in a new activity that may affect the privacy rights of individuals
7) If they need help with any contracts or sharing personal data with third parties

## The Data protection principles

7. Data Protection is based on seven principles. These are that data must be;

i. Processed lawfully, fairly and in a transparent manner.
ii. Collected for specified, explicit and legitimate purposes.
iii. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
iv. Accurate and, where necessary, kept up to date.
v. Kept for no longer than is necessary for the purposes for which it is processed.
vi. Processed in a way that ensures it is appropriately secure.

8. The further principle of accountability ties these together by requiring an organisation to take responsibility for complying with the other six principles, including having appropriate measures and records in place to be able to demonstrate compliance. This policy sets out how the Foundation aims to comply with these key principles.

**Processing personal data**

9. The Foundation will only process personal data where one of six 'lawful bases' (legal reasons) under data protection law applies:

i. The individual (or their parent/carer when appropriate) has freely given clear **consent**

ii. The data needs to be processed so that the Foundation can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract

**iii.** The data needs to be processed so that the Foundation can **comply with a legal obligation**

iv. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

v. The data needs to be processed so that the Foundation, as a charity, can perform a task **in the public interest**

**vi.** The data needs to be processed for the **legitimate interests** of the Foundation or a third party (provided the individual's rights and freedoms are not overridden)

10. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in data protection law. These are where:

i. The individual (or their parent/carer, where appropriate) has **given explicit consent;**

ii. It is necessary for the purposes of carrying out the **obligations and exercising specific rights** of the controller or of the data subject in the field of **employment** of a Data Controller or of a Data Subject.

iii. It is necessary to protect the **vital interests** of the Data Subject;

iv. Processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.**

v. The Personal Data has **manifestly been made public** by the Data Subject;

vi. There is the **establishment, exercise or defence of a legal claim**;

vii. There are reasons of **public interest** in the area of **public health**;

viii. Processing is necessary for the purposes of preventative or occupational medicine (e.g. for the **assessment of the working capacity of the employee**, the medical diagnosis, the provision of health or social care or treatment);

ix. There are **archiving** purposes in the **public interest**;

x. Where we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a privacy notice. These privacy notices can be found in a location accessible and relevant to the data subjects, including the Foundation website.

11. We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data via our privacy notices. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

12. Employees must only access and process personal data where it is necessary to do their jobs.

13. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

14. When personal data is longer required, employees must ensure it is destroyed. This will be done in accordance with the school document retention policy, which states how long particular documents should be kept, and how they should be destroyed.

## Sharing personal data

15. In order to efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but not limited to situations where:

- There is an issue which puts the safety of our staff at risk
- We need to liaise with other agencies or services – we may seek consent when appropriate before doing this where possible.
- Our suppliers or contractors need data to enable us to provide services to our employees – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law and have satisfactory security measures in place.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

16, We will also share personal data with law enforcement and government bodies when required to do so, these include but are not limited to:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or employees.

## Transferring Data Internationally

17. We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

18. We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside the EEA. The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data. For organisations which process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk. Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

## Individuals' Data Protection Rights

19. Individuals have a right to make a **'subject access request'** to gain access to personal information that the Trust holds about them. If you make a subject access request, and if we do hold information about you, we can:

i. Give you a description of it.

ii. Tell you why we are holding and processing it, and how long we will keep it for.

iii. Explain where we got it from, if not from you.

iv. Tell you who it has been, or will be, shared with.

v. Let you know whether any automated decision-making is being applied to the data, and any consequences of this.

vi. NOT provide information where it compromises the privacy of others.

vii. Give you a copy of the information in an intelligible form.

20. When responding to requests, we will not disclose information if it:

i. Might cause serious harm to the physical or mental health of an individual; or

ii. Would reveal that a child/vulnerable adult is at risk of abuse, where the disclosure of that information would not be in the child's/vulnerable adult's best interests; or

iii. Is contained in adoption or parental order records;

iv. or Is given to a court in proceedings concerning the child

21. You may also:

i. Withdraw your consent to processing at any time, this only relates to tasks which the Trust relies on consent to process the data.

ii. Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied

iii. Prevent the use of your personal data for direct marketing

iv. Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.

v. Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.

vi. Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

vii. Request a cease to any processing that is likely to cause damage or distress

viii. Be notified of a data breach in certain circumstances

ix. Refer a complaint to the ICO

x. Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

22. In most cases, we will respond to requests within 1 month, as required under data protection legislation However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances. We reserve the right to verify the requester's identification by asking for Photo ID, if this proves insufficient then further ID may be required. If the request is manifestly unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which would only take into account administrative costs. A request will be deemed to be manifestly unfounded or excessive if it is repetitive or asks for further copies of the same information. In the event we refuse a request, we will tell the individual why, and tell them they have the right to refer a complaint to the ICO.

23. The Foundation will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, individuals are asked to preferably submit their request in written format to assist with comprehension. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the request

24. If you would like to exercise any of the rights or requests listed above, please contact a Trustee. If staff receive a subject access request, they must immediately forward it to a Trustee.

25. An individual's data belongs to them therefore a child's data belongs to that child, and not the child's parents or carers. However, children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of invoking a data request. Therefore, for children under the age of 12 most data requests from parents or carers of children may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis. Where a child is judged to be of sufficient age and maturity to exercise their rights and a request is invoked on their behalf, we would require them to give consent to authorise the action to be undertaken.

## Photographs and videos

26. As part of our Foundation activities, we may take photographs and record images of individuals engaged in Foundation activities. This includes but is not limited to:

- On notice boards and in brochures, newsletters and prospectuses.
- Use by external agencies and partners such as photographers, local and national newspapers and other local and national media
- Online on our website or social media pages

27. We will obtain consent from the responsible individuals to use children's or vulnerable adults' images. When doing so we will clearly explain how the photograph and/or video will be collected and used to both the parent/carer and child/vulnerable adult when obtaining consent. Consent can be refused or withdrawn at any time. If consent is

withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child or vulnerable adult, to ensure they cannot be identified.

## Data protection by design and default

28. We will put measures in place to show that we have integrated data protection into all our data collection and processing activities. These include, but are not limited to the following organisational and technical measures:

1) Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
2) Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection regulations.
3) Completing data privacy impact assessments where the Foundation's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies or processing tools. Advice and guidance will be sought from the DPO.
4) Integrating data protection into internal documents including this policy, any related policies and privacy notices
5) Regular training for the Foundation workforce on data protection law, this policy and any related policies and any other data protection matters. Records of attendance will be kept ensuring that all data handlers receive appropriate training.
6) Periodic audits will be undertaken to monitor and review our privacy measures and make sure we are compliant.
7) Maintaining records of our processing activities, including:
    a) For the benefit of data subjects, making available the name and contact details of our Foundation DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    b) For all personal data that we hold; maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

## Data security and storage of records

30. We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. Our organisational and technical measures include, but are not limited to;

i. Paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain personal data will be kept under lock and key when not in use. We endorse a clear desk policy.

ii. Papers containing confidential personal data will not be left out on display when not in use unless there is a compelling lawful basis to do so.

iii. Passwords that are at least eight characters long containing letters and numbers are used to access Foundation computers, laptops and other electronic devices. Employees are reminded to change their passwords at regular intervals.

iv. Encryption software is used to protect any devices such as Laptops, Tablets and USB Devices where saving to the hard drive is enabled.

v. Employees or Trustees who store personal information on their personal devices are expected to follow the same security procedures as for Foundation-owned equipment.

vi. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

## Disposal of records

31. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will be rectified or updated, unless it is no longer of use and therefore will be disposed of securely. For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Foundation's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and provide a certificate of destruction. When records are disposed of as part of the Data Retention schedule this is then recorded on our record of destruction log.

## Personal data breaches

32. The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. All potential or confirmed Data Breach incidents should be reported to the Chair. They will be assigned a unique refence number and recorded in the Foundation's data breach log. Once logged, incidents will then be investigated, the potential impact assessed, and appropriate remedial action undertaken. The DPO will be consulted as required. Where appropriate, we will report the data breach to the ICO and affected Data Subjects within 72 hours. The full procedure is set out in the Foundation's Data Breach Management Policy.

33. Examples of a Data Protection Breach include but are not limited to:

- Personal data being let unattended in a meeting room
- Sending information relating to a child or vulnerable adult to the wrong employee
- A non-anonymised dataset being published on the Foundation website
- Safeguarding information being made available to an unauthorised person
- The theft of a Foundation laptop containing non-encrypted personal data about employees

## Monitoring arrangements

34. The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work, they carry out. He or she will work with the Trustees to ensure that this policy remains appropriate. This policy will be reviewed regularly, and changes recommended when appropriate. The Managing Trustees will be asked to sign off the policy review and any necessary changes.

Adopted by a meeting of the Trustees on 1st February 2023