GDPR Policy

Updated Sept 23
Review date Sept 24

Associated documents:
Links to:
Statutory guidance The UK GDPR Freedom of Information Act **Non-statutory guidance** ICO Guide to Data Protection

Contents

1. **Policy statement**
2.

a) The Dare2Dream Foundation (referred to forthwith as 'the Foundation') is committed to protecting the rights and privacy of individuals, including children and young people, staff, Board Members and parents/carers, in accordance with the UK General Data Protection Regulation (UK GDPR).
b) This Policy sets out the basis on which we will process any personal data we collect from data subjects or that is provided to us by data subjects or other sources.
c) Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our children and young people, workforce, parents and others. This makes us a data controller in relation to that personal data.
d) We are committed to the protection of all personal data and special category personal data for which we are the data controller.
e) The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.
f) All Foundation Senior Management Team and employees must comply with this Policy when processing personal data on our behalf. Any breach of this Policy may result in disciplinary action.
g) All staff have annual training on their roles and responsibilities for protecting personal data. Children and young people are also advised how to keep their information safe.

2. Data protection principles

There are six 'principles' of UK GDPR that we have to adhere to when processing personal data. We must and will ensure it is:

a) Processed fairly, lawfully and in a transparent manner.
b) Used for specified, explicit and legitimate purposes.
c) Used in a way that is adequate, relevant and limited.
d) Accurate and kept up to date - we will take reasonable steps to destroy or amend inaccurate or out-of-date data.
e) Kept no longer than is necessary - we will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.
f) Processed in a manner that ensures appropriate security of the data.

3. Basis for processing

Legislation is not intended to prevent processing personal data but to ensure it is done fairly and without adversely affecting the rights of the data subject. For data to be processed fairly, data subjects must be made aware:

a) That the personal data is being processed.
b) Why the personal data is being processed.
c) What the lawful basis for processing is.
d) Whether the personal data will be shared with third parties and if so with whom.
e) How long it is being kept for.
f) Of their rights in relation to the processing of personal data.
g) How the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.
h) Whether the personal data will be transferred outside the European Economic Area ('EEA') and if so the safeguards in place.
i) Of the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making.
j) How to raise a complaint with the Information Commissioners Office in relation to the processing.

4. Legal processing activity

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the data protection legislation. The Foundation will normally process personal data under the following legal grounds:

a) Where it is necessary for the performance of a contract with the data subject e.g. employment contract.
b) Where it is necessary to protect the vital interest of a data subject or another person.
c) Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest e.g. the Education Act 2011.
d) Where it is necessary for compliance with a legal obligation e.g. not an action in the normal course of educating children and young people.
e) Where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.

5. Processing in line with the data subject's rights

The Foundation will process all personal data in line with data subject's rights in particular:

a) The right to be informed what information we hold.
b) The right of access to any personal data.
c) The right to rectification if information is inaccurate.
d) The right to erasure.
e) The right to restrict processing of their personal data.
f) The right to data portability; having data transferred.
g) The right to object to the processing of personal data.
h) Rights in relation to automated decision making and profiling.

6. Special category personal data

When special category personal data **(see definition in Appendix 1)** is being processed then
an additional legal ground must apply to that processing. The Foundation will normally only process special category personal data under the following legal grounds:

a) Where the processing is necessary for employment law purposes, for example in relation to sickness absence.
b) Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment.
c) Where the processing is necessary for health or social care purposes, for example in relation to children and young people with medical conditions or disabilities.
d) Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

The Foundation will also ensure that only relevant and necessary information is being gathered.

The Foundation will also inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a student joins us.

If any data user is in doubt as to whether they can use any personal data for any purpose, then they must contact the Data Protection Officer (DPO) before doing so.

7. Vital interests

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing.
The Foundation believes that this will only occur in very specific and limited circumstances. In such circumstances The Foundation would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

8. Consent

If the Foundation does not have a legal basis for processing data (described above) it will ensure consent has been obtained from the data subject. The Foundation will generally seek consent directly from a child and whilst the GDPR does not set an age-related limit, the Foundation deems this to be when they reach Year 9 (12/13-year-olds).
However, the Foundation recognises that in certain circumstances this may not be appropriate and therefore may seek consent from an individual with parental responsibility for that pupil.

In relation to children and young people below Year 9, the Foundation will seek consent from an individual with parental responsibility for that student. If consent is needed, the Foundation will:

a) Inform the data subject of exactly what the Foundation intends to do with the information.
b) Require them to positively confirm that they consent – the Foundation cannot ask them to opt-out rather than an opt-in. Consent must be freely given and as a rule the Foundation will rely on written consent, however consent may occasionally be given verbally (e.g. in the case of ad-hoc photos). The Foundation will always record that this has been given.
c) Inform the data subject of how they can withdraw their consent and how this can be done.
d) Keep a record of any consent, including how it was obtained and when.

The Foundation understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

9. Information gathered

The Foundation needs to gather and process certain information to enable us to provide education and other associated functions for various purposes such as, but not limited to:

a) The recruitment and payment of staff
b) The safety of children and young people and staff
c) The administration of programmes of study and courses and allocating the correct teaching resource
d) Pupil enrolment
e) Examinations and external accreditation
f) Recording pupil progress, attendance and conduct
g) Collecting fees
h) Complying with legal obligations to funding bodies (e.g. the Local Authority).

The Foundation collects this information in a variety of ways including but not exclusively from:

- Registration forms
- Medication forms
- Common Transfer Files (CTFs) from previous Foundations
- Staff contract information
- Child protection plans
- Board Member information.

The Foundation may contract with various organisations who provide services to the it including, but not exclusively:

- Payroll providers
- Pension providers
- DBS check providers
- Occupational Health
- Legal advice
- Recruitment providers
- Management Information Systems
- Education Welfare and services from the Local Authority
- Parent portals/communication systems to enable us to effectively communicate with parents
- Foundation trip recording
- Safeguarding recording
- HR systems for effective management of staff

In order that these services can be provided effectively The Foundation is required to transfer personal data of data subjects to the data processors.

Personal data will only be transferred to a data processor if they agree to comply with the Foundation's procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Foundation. The Foundation will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.
Contracts with data processors will comply with data protection legislation and contain explicit obligations on the data processor to ensure compliance with the data protection legislation, and compliance with the rights of data subjects.

The Foundation will inform data subjects of any sharing of their personal data unless The Foundation is not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

In some circumstances the Foundation will not share safeguarding information. Please refer to the Safeguarding Policy.

10. Data protection impact assessments

In certain circumstances the law requires the Foundation to carry out detailed assessments of proposed processing. This includes where it intends to use new technologies which might pose a high risk to the rights of data subjects because of the number of people that this might affect, types of data it will be processing or the way that it intends to do so.

The Foundation will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered. The CEO serves as the Data Protection Officer and should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

11. Data Controller and Data Protection Officer

The Foundation is the 'data controller' under the terms of the legislation – this means that it is ultimately responsible for controlling the use and processing of personal data. The Data Protection Officer (DPO) for the Foundation is the CEO can be contacted at the Foundation.

The DPO is responsible for ensuring compliance with the data protection legislation and with this Policy. The CEO is also responsible for all day-to-day data protection matters, ensuring that all members of staff, contractors, short-term and voluntary staff and visitors receive training and abide by this Policy and for developing and encouraging good information handling throughout the Foundation.

12. Expectations of staff

All staff must ensure that:

a) All personal data is kept securely, and personal data is locked in drawers/cupboards.
b) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.
c) Individual monitors do not show confidential information to passers-by.
d) Paper documents should be shredded in a cross-cut shredder or via secure disposable waste systems. ICT assets must be disposed of in accordance with ICT related policies.
e) Electronic devices must be password protected and locked when not in use.
f) Documents must be collected immediately from printers and photocopiers.
g) Professional email etiquette must be maintained at all times.
h) Personal data is provided and retained appropriately.
i) Any queries regarding data protection, including subject access requests and complaints, are promptly advised to the CEO (DPO).
j) Any data protection breaches are swiftly brought to the attention of the CEO (DPO) and that staff are instrumental in resolving breaches.
k) Where there is any uncertainty around a data protection matter advice is sought from the CEO (DPO).

13. Photographic images

a) Where a person is identifiable, photography and videography footage is classified as 'personal data'. In some instances, the processing of such personal data can also be classified as 'sensitive personal data', for example revealing racial or ethnic origin, political opinions, religious or philosophical beliefs.
b) This Policy is concerned with ensuring that the Foundation operates within current legislation and adopts best practice as regards to capturing and storing photography or videography for official use.
c) This Policy does not apply to photography and videography captured for solely personal use by individuals such as children and young people, parents, carers,

and family members of children and young people, for example, a parent taking images of their child in a Foundation event. Parents/carers and other individuals attending the Foundation events will be asked that they do not post any images or film footage which include any child other than their own child on any social media, or otherwise publish those images or film footage, without the permission of the parents/carers of any other identifiable children.

d) Photographs or film footage of crowds are not classified as personal data, providing no one person is the focus of the image. Crowd photographs which are cropped to focus on one individual will however be defined as personal data.
e) Images and film are powerful tools to capture and convey the spirit of being part of the Foundation – positively depicting our shared values and promoting and celebrating the many achievements of our community.
f) The protection of our children and young people is also paramount, and this Policy sets out the framework within which the Foundation operates to ensure the safe, secure and appropriate use of photography and film in a range of settings.
g) Photography and videography is used to capture people, places and events. The range of official uses include, but are not limited to:
    - personal identity cards
    - student records, curriculum and course work
    - display boards
    - websites and social media accounts
    - promotional literature and communications (print and digital formats)
    - press and media
h) Care is taken to reduce the risk that images could be misused by others outside of the Foundation. In general, photography and film footage will not include captions or names which specifically identify individuals. Where additional personal data is necessary to accompany an image, this will be limited, for example, to a first name only.
i) Parental/carer or pupil (as appropriate) permission is obtained via the Foundation to which the individual pupil is registered – strictly following the Foundation data consent process. The record of this will be held on the Foundation management information system (MIS), to ensure consent for a child or young person to be photographed and filmed is consistently and accurately documented.
j) Consent can be withdrawn at any time by in writing, directly contacting the Foundation. Once consent is withdrawn, the Foundation will not use the relevant images again, but it will not normally be possible to recall publications in which their image has already appeared.
k) In some scenarios, the Foundation has a 'legitimate interest' to use imagery in support of safeguarding and in delivering a child's education, and which does not cause the identified individual unwarranted prejudice, damage or distress. In such instances, explicit consent is not required. Examples include displays, pupil records and academic work.
l) The Foundation may use staff and/or external professional photographers and videographers in capturing imagery.
m) Where photography and film are captured by Foundation staff, only Foundation equipment and devices will be used.

n) External contractors may use their own equipment and devices to capture imagery in compliance with current legislation and this Policy.
o) Careful consideration must be given when capturing images and footage, to ensure that:
    1. Children and young people are suitably clothed to reduce the risk of inappropriate use; for example, particular attention is given to settings such as sports, swimming and drama.
    2. Appropriate camera angles are used; and children and young people are not captured in a position of 'vulnerability', such as emotional distress, upset or embarrassment.
    3. Children and young people are not named within the image itself.
    4. External photographers/videographers are not left with unsupervised access to children and young people.
    5. Photography sessions are not held outside a Foundation event or at a pupil's home.
    6. Before taking a photograph, verbal permission is sought, therefore giving anyone who does not wish to be included the opportunity to opt out; noting this does not supersede the need for written consent as outlined earlier in this Policy.

p) Digital images and film footage must be transferred to a secure location at the earliest opportunity, this can be any Foundation network folder with appropriate restricted access and the host device files must be wiped. Devices and equipment must be regularly checked and cleared of files to ensure adherence to this Policy.
q) Where third-party platforms are used to support the transfer of files, relevant due diligence must be carried out to ensure sufficient security and legislative compliance is in place before using.
r) Images and film footage cannot be stored on portable equipment such as memory sticks, removable hard drives and mobile phones. Storing personal information on these devices is not considered secure.
s) Hard copy images, where retained, must be stored in a locked draw with restricted access.
t) Images and film footage must be stored in dated and annotated file folders (or a digital photography library).

15. CCTV

a) Any CCTV system's design and extent, its general use and management are undertaken to ensure they provide the required level of cover for each individual situation, however the Foundation will follow the guiding principles set out within this Policy.
b) Children and young people, staff and members of the public using these facilities are safeguarded the facilities are secure to deter anti-social or illegal activity on our premises said the police to identify persons if an offence is committed.
c) Systems will be will be installed and managed in accordance with the principles and objectives expressed in the ICO Code of Practice.
d) Each CCTV system is registered with the Information Commissioners Office under the terms of the General Data Protection Regulations (GDPR).

e) The day-to-day management of the system will be the responsibility of the CEO with the support of the Site Owner.
f) The CCTV systems will be operated 24 hours each day, all year round.
g) Where systems are capable of recording audio it should be muted as normal practice. Where audio is recorded this should only be for very specific reasons.
h) Only the CEO or member of the Senior Management Team can request access to view information/images in the event of an incident or situation occurring.
i) CCTC system protocols that will be observed are as follows:
    - The CCTV systems are closed digital systems.
    - Warning signs will be placed throughout the premises where the CCTV system is active.
    - The CCTV system has been designed for maximum effectiveness and efficiency. The Foundation cannot however guarantee that every incident will be detected or covered and 'blind spots' may exist.
    - The CCTV system will not be trained on individuals unless an immediate response to an incident is required.
    - The CCTV system will not be trained on private vehicles or property outside the perimeter of the Foundation.
    - Access to the system will be strictly limited to those staff already noted.
    - Images/recorded data can only be viewed with authorised consent of those staff noted and recorded within the CCTV register.
    - All stored data will be kept in a secure locked area or via password protected access to a secure server.
    - Recordings will only be released following submission of a formal request as specified below on the authority of the CEO or Foundation Proprietor (the support of the Site Owner may be required to facilitate this) then only to the Police or as required under a Subject Access Request.
    - The Foundation may choose to use visual display screens; these may generally be within reception or similar areas to ensure access to the site and main doors are monitored during operational hours. These screens should not be visible to children and young people or members of the public.
    - Images will only be retained for as long as they are required.
    - Images will only be used for the purposes for which it is intended, including supporting public safety, protection of children and young people, staff and law enforcement.

j) Individuals whose personal data is recorded on Foundation CCTV have a right to make a Subject Access Request to be provided with that information or, if they consent to it, view that information. Information must be provided within the specified ICO timeline of one calendar month upon receiving a request.
k) Subject Access Requests can be made verbally but personal identification will always be requested and therefore the request submitted in writing, either by letter or emails via the Foundation to the CEO (DPO) via email: enquiries@thedare2dreamfoundation.org.uk.
l) Coordination to meet the specified timelines of a Subject Access Request, keeping the DPO informed of progress, seeking guidance as required will be the responsibility of the CEO (DPO).

m) Subject Access Requests that are made in writing should include:
    1. Name of individual.
    2. Date and time that the request was made.
    3. Correspondence address.
    4. Contact number and email address.
    5. Details of the information requested with specific time periods where applicable.

n) Footage should only be provided once viewed by the CEO (DPO) to ensure that it does not contain third party information.
o) Complaints about the CCTV systems should be addressed to the CEO (DPO) in the first instance. If the complainant wishes to pursue the matter further the Foundation Complaints Policy is available on the Foundation website.

16.Recruitment and Selection

The Dare2Dream Foundation recruits staff to work in all areas of the Foundation. All recruitment follows Safer Recruitment (see Safer Recruitment Policy)

Below are the directives of GDPR that the Foundation takes when recruiting staff:

- The Foundation will only collect data that it needs for legitimate interest to process candidate data**.** GDPR obliges that the collection of data is only for "specified, explicit and legitimate purposes." This means that the foundation will only source candidate data which is job-related information only and is intended for purposes of contacting sourced candidates within 30 days.
- Consent is requested by the candidate to process sensitive data**.** When processing data such as disability information, cultural, genetic or biometric information or information gathered for the background check consent is required. The use of external registered organisations such as for DBS checks requires that consent is given by the candidate before submitting the sensitive data. Candidates have the right to withdraw their consent should they wish to, however, this may affect the employment offer if suitable checks for working with children and young people cannot be carried out due the withdrawal of consent.
- The Foundation have clear privacy policies and use recruitment sites that also adhere to these policies, the data collected will only be used for recruitment purposes only.

Candidates are able to exercise their rights under GDPR:

- Candidates have the "right to be forgotten." All Candidates have the right to ask the Foundation to delete and stop processing their personal data. In this instance written requests are required and as such all data will be deleted in any sources that the information is held, within one month after receiving the candidate's request.

- Candidates have the right to access their data and ask you to rectify it. Candidates have the right to ask what data of theirs you hold. They can also request that you make corrections to any inaccuracies (rectify.) The Foundation will grant both requests within one month and provide candidates with a free, electronic copy of their own personal data.

All unsuccessful candidates including those that offers have been withdrawn will be removed from The Foundation databases and accompanying systems within 180 days. Any exceptions to this may be in the case that the candidate has been referred to safeguarding or legal processes due to information received during the recruitment and selection process.

17. Record Retention

See appendix 3 for retention periods of all children and young people, staff and candidates records.

16. Subject access requests (SARs)

Any individual has a right to access personal data relating to them which is held by the Foundation by means of a Subject Access Request (SAR). Personal data is information relating to an individual and a Subject Access Request may be made in any form e.g. in hard or soft copy in writing, by social media, by email, verbally etc.

Any member of staff receiving a SAR must forward it to the CEO (DPO) in the Foundation. Under GDPR regulations, the information will be provided free of charge and the Foundation will be responded to within a calendar month.

Please refer to Appendix 2 – Subject Access Request Form.

17. Data breaches

Where a data protection breach occurs or is suspected to have occurred all staff are aware that they need to inform the CEO (DPO) who will seek to take the necessary steps to:

- Minimise the damage.
- Assess the extent of the damage and determine whether the Information Commissioners Office (ICO) should be notified
- Notify individuals affected as appropriate.
- Ascertain how the breach occurred and, if appropriate, determine how to prevent or minimise future breaches.

18. Confidential waste

Confidential waste will be securely stored and disposed of in line with good practice in records management and retention. Shredding companies who have been certified as being GDPR compliant will be used to dispose of any secure waste and a record of destruction will be retained.

19. Enquiries

Anyone who has any queries about this Policy should write to the CEO (DPO) at the following address: The Dare2Dream Foundation, 68 Albion Court, Nuneaton, CV11 4JJ. Alternatively, they can email via enquiries@thedare2dreamfoundation.org.uk

20. Complaints

Any complaints will be dealt with in the first instance according to the Foundation's Complaints Policy which can be found on the Foundation website.

If the complaint is unresolved by following this policy, any complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at:

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113

Alternatively a concern can be reported online at https://ico.org.uk/concerns.

21. Policy review

The Foundation will monitor and review the implementation and impact of this Policy yearly. This may occur earlier should there be a change in legislation, statutory guidance or an event or incident in the Foundation which makes this necessary.

Appendix 1 Definitions

Data	Information, which is stored electronically, on a computer, or in certain paper-based filing systems.
Data subjects	For the purpose of this Policy include all living individuals about whom we hold personal data. This includes children and young people, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal data	Means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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.
Data controllers	People who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data users	Those of our workforce (Foundation Board and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the 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 also includes transferring personal data to third parties.

Special category personal data	Includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Workforce	Includes, any individual employed by the Foundation such as staff and those who volunteer in any capacity including Foundation Board and volunteers.

Appendix 2 Subject Access Request Form

You can use this form to request access to the personal information held by the Foundation about you or as a parent/carer about your child(ren). If you are requesting information about your child(ren), **we will generally seek consent directly from them where it is deemed that they would understand the information being requested, why it is being requested and what the requester will be using the information for**.

Whilst UKGDPR does not set an age- related limit, as a Foundation we deem this to be from Year 9 (12/13 year olds) however, we recognise that in certain circumstances this may not be appropriate and therefore we may seek consent from an individual with parental responsibility. *Please see the authority at the end of this form.*

Under the UK General Data Protection Regulation (UKGDPR) data subjects have a right to be told whether the Foundation – or someone else on the Foundation's behalf – is processing your personal data and, if so, to be given a description of:

1. The personal data held;
2. The purposes for which that personal data is being processed;
3. Those to whom that personal data is being or may be disclosed.

Section one – your details

Surname:	
First name(s):	
Address:	
Telephone:	
Email:	
If the information relates to a pupil(s) at the Foundation, please provide the name and age of the pupil(s) about whose personal data you are requesting:	
Do you have parental responsibility for the student who is the 'Data Subject'. If the answer is 'No' please provide justification for your request:	

Appendix 3

Accident records/reports for any reportable work accident, death or injury - **Statutory retention period:** At least 4 years from the date the report was made (or until any younger person involved in the accident reaches 21).

Staff Records

GDPR doesn't set out any minimum or maximum time limits for keeping staff data, however, the Foundation is committed to not keep any records longer than is needed.

Working time records: Kept for 2 years from the date the records refer to.

Payroll records: Kept for 3 years from the end of the tax year that they relate to.

Maternity, Paternity or Shared Parental Pay records: Kept for 3 years after the end of the tax year that the payment stopped.

Immigration checks - **Statutory retention period:** 2 years after the termination of employment.

Income tax and NI returns, income tax records and correspondence with HMRC - Statutory retention period: Not less than 3 years after the end of the relevant financial year.

Retirement Benefits Schemes - **Statutory retention period:** 6 years from the end of the scheme year in which the event took place.

Statutory Maternity Pay records including Mat B1s, dates of maternity leave, certificates showing the expected week of confinement (also shared parental, paternity and adoption pay records) - **Statutory retention period:** 3 years after the end of the tax year in which the maternity period ends.

Working time records including overtime, annual holiday, time off for dependents, opt outs etc -**Statutory retention period:** 2 years from date on which they were made. Records in relation to hours worked will currently be kept for 3 years, beginning with the day on which the pay reference period ends.

Special category or personal data consents

Consents for the processing of special categories of personal and sensitive data will be retained while the data is being processed. Keeping the consents may be justified for six to seven years after employment ends.

Former staff data

After an employee leaves the Foundation, personal data, performance appraisals and employment contracts will be retained for six years after an employee leaves.

Keeping the consents may be justified for six to seven years after employment ends.

Job applicant data

Records of candidates applying for positions in the foundation or those that have been unsuccessful in their application based on outcome of interview or other factors such as unsuccessful references, records will be kept for 180 days before being removed from all Dare2Dream records including any external records used in the recruitment process such as DBS checks.

Training Records

First aid training- Statutory retention period: 6 years after employment.

Fire warden training -Statutory retention period: 6 years after employment.

Health and Safety representatives and employees' training - Statutory retention period: 5 years after employment.

Records relating to children and young adults

Statutory retention period: until the child/young adult reaches the age of 21.

Subject access request

Statutory retention period: Records will be kept as long as they are needed after the last communication concerning a subject access request

Whistleblowing documents

Statutory retention period: 6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data will be removed immediately.