Data Protection Policy

(Incl. GDPR Compliance)

Document Title	Data Protection Policy
Author	A Poole, Director of Operations
Version Number	Version 1
Approved by	TPT Board
Effective from	December 2021
Due for Revision	December 2023

Contents

Document Control Table

Document History			
Version	**Date**	**Author**	**Note of Revisions**
V1	December 2021	A Poole	First Trust-wide Data Protection policy.

1. Introduction

1.1. The Prospect Trust ("the Trust"), recognises the importance of data protection and is committed to protecting and safeguarding personal data. The Trust collects, stores and processes personal data on a variety of stakeholders in order to carry out its activities and functions.

1.2. The Trust recognises that having controls around the collection, use, retention and destruction of personal data is important in order to comply with its obligations under Data Protection laws and in particular its obligations under Article 5 of the UK General Data Protection Regulation (UK GDPR).

1.3. The Trust's Data Protection Officer is responsible for informing and advising the Trust and its staff on its data protection obligations and for monitoring compliance with those obligations and this policy. If you have any questions about the content of this policy, or if you need further information, you should contact the Data Protection Officer via email at dpo@prospecttrust.org.uk

2. About This Policy

2.1. This policy applies to the Trust and its constituent academies. References to the "Trust" should be read to include "and its Academies" as appropriate. This Policy (and the other policies and documents referred to in it) set out the basis on which the Trust, will collect and use personal data either where the Trust collects it from individuals itself, or where it is provided to the Trust by third parties. It also sets out rules on how the Trust, handles, uses, transfers and stores personal data.

2.2. This policy applies to all personal data stored electronically, in paper form, or otherwise.

2.3. This policy will be updated as necessary to reflect best practice, or amendments made to the data protection legislation, and shall be formally reviewed and approved by the Board every two years.

3. Definitions

3.1. **Personal Data** – any information that can be related to an identified or identifiable living person (referred to as a data subject).

3.2. **Special Categories of Personal Data –** personal data that reveals a person's

- racial or ethnic origin;
- political opinions:
- religious or philosophical beliefs;
- trade union membership;
- genetic data, biometric data;
- physical or mental health;
- sexual life or sexual orientation.

3.3. These special categories of personal data are subject to additional controls in comparison to ordinary personal data. Staff or students are under no obligation to disclose data under these categories (save to the extent that marital details and / or parenthood are needed for other purposes e.g. pension entitlements.)

3.4. Information relating to criminal convictions shall only be held and processed where there is a legal authority to do so.

3.5. **Controller** – any entity (e.g. company, organisation or person) that determines the purposes for which, and the manner in which, any personal data is processed. The Trust and its constituent academies are data controllers.

3.6. **Processor** – any entity (e.g. company, organisation or person) that processes personal data on behalf of a controller (e.g. the Trust).

4. Trust Staff General Obligations

4.1. All Trust staff must comply with this policy and associated staff procedures. Trust staff must ensure that they keep confidential all personal data that they collect, store, use and come into contact with during the performance of their duties. Trust staff must not release or disclose any personal data:

- outside the Trust; or
- inside the Trust to staff not authorised to access the personal data, without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

4.2. Trust staff must take all steps to ensure there is no unauthorised access to personal data whether by other Trust staff who are not authorised to see such personal data or by people outside the Trust.

5. Training

5.1. The Trust is committed to ensuring its staff undertake an appropriate level of training to help them understand their duties in relation to data protection and to ensure compliance. This training will be provided at induction and thereafter annually. Records of completion of training will be maintained.

6. Data Protection Principles

6.1. When using personal data, Data Protection laws require that the Trust complies with the following six principles which require personal data to be:

6.1.1. processed lawfully, fairly and in a transparent manner;

and processing shall not be lawful unless one of the processing conditions can be met:

6.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

6.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

6.1.4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as

soon as possible;

6.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and

6.1.6. 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.

6.2. The Trust is committed to complying with the principles in 6.1 at all times. This means the Trust will:

6.2.1. Inform individuals as to the purpose of collecting any information from them, through the use of Privacy Notices which are issued at application ;

6.2.2. Be responsible for checking the quality and accuracy of information;

6.2.3. 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 data retention guidance.

6.2.4. Ensure that when information is authorised for disposal it is done appropriately;

6.2.5. Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on the Trust's computer system, and follow the relevant security policy requirements at all times;

6.2.6. Share personal information with others only when it is necessary and legally appropriate to do so;

6.2.7. Set out clear procedures for responding to requests for access to personal information known as subject access requests;

6.2.8. Report any breaches of the UK GDPR in accordance with the procedures in section 12 below.

7. Lawful use of Personal Data

7.1. In order to collect and/or use personal data lawfully, and in accordance with the first principle defined in 6.2.1. above, the Trust needs to be able to demonstrate that its use meets one of a number of legal grounds:

7.1.1. **Consent:** the individual has given clear consent that is specific to the particular type of processing activity, and that the consent is informed, unambiguous and freely given.

7.1.2. **Contract:** the processing is necessary for a contract with the individual, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

7.1.3. **Legal obligation:** the processing is necessary for compliance with the law.

7.1.4. **Vital interests:** the processing is necessary to protect the vital interests of the

individual or another e.g. their life.

7.1.5. **Public task:** the processing is necessary to perform a task in the public interest, or in the exercise of official authority vested in the Trust.

7.1.6. **Legitimate interest:** the processing is necessary for legitimate interests of the Trust or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

7.2. In addition, when the Trust collects and/or uses special categories of personal data, it must be able to demonstrate that one of a number of additional conditions is met:

- Explicit consent;
- Employment and social security obligations;
- Vital interests;
- Necessary for establishment or defence of legal claims;
- Substantial public interest; and
- Various scientific and medical issues.

8. Transparent Processing – Privacy Notices

8.1. Where the Trust collects personal data directly from individuals, the Trust will inform them about how the Trust uses their personal data in a privacy notice. These notices are available on the Trust and individual academy websites and are subject to regular review.

9. Data Quality

9.1. Data Protection laws require that the Trust only collects and processes personal data to the extent that it is required for the specific purpose(s) notified to the individual in a privacy notice. The Trust is also required to ensure that the personal data that it holds is accurate and kept up to date.

9.2. The Trust will take reasonable steps to ensure that personal data is recorded accurately, is kept up to date and limited to that which is adequate, relevant and necessary in relation to the purpose for which it is collected and used.

9.3. The Trust will ensure that personal data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection laws.

10. Data Retention

10.1. Data Protection laws require that the Trust does not keep personal data longer than is necessary for the purpose or purposes for which the Trust collected it.

10.2. The Trust has assessed the types of personal data that it holds and the purposes it uses it for and has set retention periods for the different types of personal data processed by the Trust and the reasons for those retention periods. Please refer to the Trust or relevant Academy website for further details.

11. Data Security

11.1. The Trust takes information security very seriously and the Trust will use appropriate technical and organisational measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

12. Data Breach

12.1. A personal data breach is defined very broadly and is effectively any failure to keep personal data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of personal data.

12.2. There are three main types of personal data breach, which are as follows:

- Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems that a member of staff is not authorised to access, accessing personal data stored on a lost laptop, phone or other device, people gaining access to personal data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from backup, or loss of an encryption key; and
- Integrity breach - where there is an unauthorised or accidental alteration of personal data.

12.3. In the event that a data breach occurs, the Data Protection Officer shall co-ordinate an assessment of:

- The extent of the breach;
- The risks to the data subjects as a consequence of the breach;
- Any security measures in place that will protect the information;
- Any measures that can be taken immediately to mitigate the risk to the individuals.

12.4. Unless there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Trust.

12.5. The Information Commissioner shall be told:

- Details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- The contact point for any enquiries (which shall usually be the Data Protection Officer);
- The likely consequences of the breach;
- Measures proposed or already taken to address the breach.

12.6. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Principal of the relevant academy, or in the case of the Trust, the Trust Executive, shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

12.7. Data subjects shall be told:

- The nature of the breach;
- Who to contact with any questions
- Measures taken to mitigate any risks.

12.8. The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Trust Executive Team and a decision made about implementation of those recommendations.

12.9. All data breaches shall be recorded in the Trust's Data Breach Log.

13. Data Processors

13.1. When appointing an external data processor, the Trust will ensure that appropriate contracts are in place.

13.2. Contracts with external organisations must provide the following obligations as a minimum:

- to only act on the written instructions of the controller;
- to not export personal data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the controller and under a written contract;
- to keep the personal data secure and assist the controller to do so;
- to assist with the notification of data breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals rights;

- to delete/return all personal data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the UK GDPR.

13.3. In addition, the contract should set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of individuals; and
- the obligations and rights of the controller.

14. Individuals' Data Processing Rights

14.1. Individuals have rights with regards to how their data is processed. These rights include to:

- withdraw Consent to processing at any time;
- receive certain information about the Data Controller's processing activities;
- request access to their Personal Data that the Trust hold (Subject Access Request);
- prevent the use of their Personal Data for direct marketing purposes;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling (Automated Decision Making);
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority (the ICO); and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

14.2. The Trust is required to verify the identity of an individual requesting data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

14.3. The Trust is responsible for ensuring that a process is in place to ensure that

personal data remains up to date and accurate.

14.4. Individuals are responsible for helping the Trust to keep their personal data up to date. Individuals should let the Trust know if the information they have provided to the Trust changes.

14.5. The Trust will use all personal data in accordance with the rights given to individuals under Data Protection laws.

15. Other rights of individuals

15.1. The Trust has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the Trust will comply with the rights to:

- object to processing;
- rectification;
- erasure; and
- data portability

Right to object to processing

15.2. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are valid.

15.3. Where such an objection is made, it must be sent to the Trust DPO upon receipt, and the DPO will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

15.4. The DPO shall be responsible for notifying the individual of the outcome of their assessment at the earliest opportunity, but as a maximum within one month.

Right to rectification

15.5. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the DPO immediately on receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

15.6. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a, review under the data protection complaints procedure, or, an appeal direct to the Information Commissioner.

15.7. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

15.8. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- Where consent is withdrawn and there is no other legal basis for the processing;
- an objection has been raised under the right to object, and found to be legitimate;
- personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
- Where there is a legal obligation on the Trust to delete.

15.9. The Data Protection Officer will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

15.10. In the following circumstances, processing of an individual's personal data may be restricted:

- Where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;
- Where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- Where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;
- Where there has been an objection made, pending the outcome of any decision.

Right of data portability

15.11. An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format where the processing is:

- based on consent or on a contract; and
- carried out by automated means.

15.12. This right isn't the same as subject access and is intended to give individuals a subset of their data.

16. Subject Access Requests

16.1. Individuals have the right under the UK GDPR to ask the Trust to confirm what personal data they hold in relation to them and to provide them with the data. Such requests can be made to any member of staff who should immediately inform the DPO.

16.2. Requests can be verbal or in writing and a response must be provided within one month, this can be extended by a further 2 months for complex requests. The individual should be advised if this will be the case.

16.3. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 13, or over 13 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Academy Principal must, however, be satisfied that:

- the child or young person lacks sufficient understanding; and
- the request made on behalf of the child or young person is in their interests.

16.4. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Academy/Trust must have written evidence that the individual has authorised the person to make the application and the Academy/Trust must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

16.5. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

16.6. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

16.7. All files must be reviewed by the Trust Executive or Academy Principal before any disclosure takes place. Access will not be granted before this review has taken place.

16.8. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

17. Marketing and Consent

17.1. Where the Trust carries out marketing, Data Protection laws require that this is only done in a legally compliant manner; consent will be obtained where appropriate.

18. Automated Decision Making and Profiling

18.1. Under Data Protection laws there are controls around profiling and automated decision making in relation to individuals.

- **Automated Decision Making** - happens where the Trust makes a decision about an individual solely by automated means without any human involvement and the decision has legal or other significant effects; and
- **Profiling** - happens where the Trust automatically uses personal data to evaluate certain things about an Individual.

18.2. Where the Trust uses automated decision making or profiling, the data subject will be informed in the appropriate privacy notice and has a right to object.

19. Privacy by Design and Data Protection Impact Assessment (DPIA)

19.1. The Trust is required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

19.2. This means that the Trust must assess what Privacy by Design measures can be implemented on all programs/systems/processes that process Personal Data by taking into account the following:

- use of most appropriate systems and procedures;
- the cost of implementation;
- the nature, scope, context and purposes of processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

19.3. The Trust is also required to conduct DPIAs in respect to high risk processing.

19.4. The Trust and its academies should conduct a DPIA when implementing major system or business change programs involving the processing of Personal Data including (but not limited to):

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated processing including profiling and automated data management;
- large scale processing of Sensitive Data; and
- large scale, systematic monitoring of a publicly accessible area.

19.5. A DPIA will also be undertaken as a matter of good practice to help assess and mitigate the risks to individuals. If processing is likely to result in a high risk to the rights and freedom of children then a DPIA should be undertaken.

19.6. A DPIA must include:

- a description of the collection, processing and use of personal data, its purposes and the legal basis for processing if appropriate;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to the rights and freedoms of individuals; and
- the risk mitigation measures in place and demonstration of compliance.

19.7. All DPIAs will be reviewed by the Data Protection Officer and the Academy/Trust senior leadership/executive will make a decision to proceed informed by DPO advice..

20. Enquiries

20.1. Further information about the Academy's Data Protection Policy is available from the DPO.

20.2. General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk