Waterloo Primary Academy

Data Protection Policy

Approved & Adopted: 19 June 2018
Responsible Personnel: N Lea
Policy Last Reviewed/Approved: February 2023
Review Period: Annual
Review Date: February 2024

Zest Academy Trust

You must read this policy because it gives important information about:

- the data protection principles with which the Trust must comply
- what is meant by personal information (or data) and sensitive personal information (or data)
- how we gather, use and (ultimately) delete personal information and sensitive personal information following the data protection principles
- where more detailed privacy information can be found, e.g. about the personal information we collect and create, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached declaration (page 14) to Nicola Lea HR Business Manager

Introduction

Zest Academy Trust (hereafter "the Trust") aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed following the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (the Act).
The Trust must notify staff, governors and others who work for or on behalf of the Trust of the information contained in this policy.
This policy applies to current and former employees, Trustees, volunteers and others who work for and on behalf of the Trust. If you fall into one of these categories, please read this policy alongside your contract of employment (or contract for services) and any other notice the Trust issues from time to time relating to the processing of personal data.
This policy does not form part of your contract of employment (or contract for services if relevant) and may be amended by the Trust at any time.
This policy explains how the Trust will hold and process personal data. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Trust.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

This policy meets the requirements of the UK GDPR and the provisions of the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR, and the ICO's code of practice for data sharing.
It also reflects the Surveillance Camera Commissioner's Code of Practice for the use of surveillance cameras and personal information.
This policy also complies with the Trust's funding agreement and Articles of Association.

Definitions

Data subject
An individual to whom such personal data relates.

Data controller
The data controller is the body that is responsible for storing and controlling personal data. Zest Academy Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Data processor
A data processor is a person, other than an employee responsible for processing personal data on behalf of a controller.

Personal data
Personal data is information relating to an individual where they 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.
Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to an individual.

Special category data
Special categories of personal data refer to an individual data subject's, race, ethnic origin, political view, religion, trade union membership, genetics and/or biometric data used to uniquely identify an individual, health data, or concerning an individual's sex life or sexuality.

Criminal records information
Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

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

Processing
any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, 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.

Roles and responsibilities

This policy applies to all staff, volunteers and others working for or on behalf of the Trust. Staff who do not comply with this policy may face disciplinary action.

Governing board
The governing board has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

Data Protection Officer
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The DPO will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Trust data protection issues. The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO. Full details of the DPO's responsibilities are set out in the Service Level Agreement.

Our DPO is The Schools People and is contactable by emailing

DPOService@Schoolspeople.co.uk

Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

All staff

Staff are responsible for:

- Collecting, storing and processing personal data following this policy.
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the United Kingdom
    - If there has been a data breach
    - Whenever they are engaging in a new processing activity or procuring a new third-party service provider that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

Data Protection Principles

The UK GDPR is based on data protection principles that the Trust must comply with. The principles say that personal data must be:

1. processed lawfully, fairly and in a transparent manner
2. processed for a specific, explicit and legitimate purpose
3. adequate, relevant and limited to what is necessary for the purpose for which it is being processed
4. accurate and, where necessary, kept up to date
5. kept for as long as necessary for the purpose for which the data is processed
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical or organisational measures

These Principles are further strengthened by the Accountability principle which requires the Trust to evidence its compliance with the UK GDPR.

This policy sets out how the Trust aims to comply with these principles.

Processing Personal Data: Lawfulness, Fairness and Transparency

We will only process personal data where there are one or more 'lawful bases' (legal reasons) to do so under data protection law, including

- compliance with a legal obligation.
- the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.
- for the performance of a contract with the data subject or to take steps to enter into a contract.
- protecting the vital interests of a data subject or another person.

Where the Trust is not operating in its capacity as a public authority, for example in providing after-school activities or facilities hire, the lawful basis for that processing will be legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.
When processing 'special category'data (see 'Definitions', above), the Trust will identify an additional condition for the processing set out in Article 9 (2) of the UK GDPR, where processing is necessary for:

- protecting the vital interests of the individual where they are physically or legally incapable of giving consent
- to carry out rights and obligations under employment law
- the assessment of a person's working capacity either based on UK Law or under contract with a health professional such as an occupational health provider
- the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity
- reasons of substantial public interest, based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- reasons of public interest in the area of public health
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- the data has been manifestly made public by the individual e.g., on social media.

Additionally, the Trust may also require a further condition specified in Schedule 1 to the Data Protection Act (2018) to process certain types of special category data. See Appendix 1: *Appropriate Policy Document* for further information and guidance.

Consent

Where no lawful basis for processing exists, the Trust must seek consent for that processing. For example, where the Trust wishes to use images of individuals in marketing publications or on social media channels, written consent must be obtained.

Consent is defined as: “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (UK GDPR Article 4(11)).
Consent must be a positive indication, it cannot be inferred from silence, inactivity or pre-ticked boxes.
Where the processing is based solely on consent the Trust shall be able to demonstrate that the data subject, or their representative (e.g., parent/carer in the case of a pupil), has provided consent to the processing of their personal data.
The data subject or their representative has the right to withdraw their consent at any time and shall be informed of this right before providing their consent. This does not affect the lawfulness of the processing before consent was withdrawn.
If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as the basis for processing, we will obtain parental consent where the pupil is under 13 (except for online counselling and preventive services).

Criminal Convictions and Offences

The Trust may use information relating to criminal convictions where the law and our policies allow us to do so.
The Trust will hold information about criminal convictions if information about criminal convictions becomes apparent during a stakeholder’s relationship with us.
Information about criminal convictions and offences will be used in the following ways:

- to ensure an individual's suitability to work
- to ensure a staff member’s suitability to drive the Academy minibus
- for safeguarding purposes.

Less commonly, information relating to criminal convictions may be used where necessary in relation to legal claims; where it is necessary to protect an individual’s vital interests (or someone else’s vital interests) and they are not capable of giving consent, or where information has already been made public.

Processing Personal Data: Limitation, Minimisation and Accuracy

The Trust 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.
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.
Personal data will be adequate, relevant and limited to what is necessary to fulfil the purpose for which it is collected and otherwise processed
The Trust will take reasonable measures to ensure that all personal data is accurate and kept up to date.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done following the Trust’s *Data Retention Schedule*.

Sharing Personal Data

The Trust will not share personal data with third parties, without consent, unless the law and our policies allow us to do so.

Statutory Obligations

The Trust is required, by law to pass certain information to specified external bodies, to meet its statutory obligations. Examples of organisations with whom personal data may be shared regularly include, but are not limited to:

- Department for Education
- The Local Authority
- Ofsted
- Disclosure and Barring Service
- HMRC
- Teachers' Pension Service
- Local Government Pension Service

Third-party contractors/service providers

Our suppliers and/or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies, HR Consultants, Occupational Health Services, Payroll, Wellbeing Services, etc.

When selecting companies and contractors to work with, the Trust will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection legislation
- Establish a data-sharing agreement (DSA) 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 shared with them
- 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

The Trust requires these companies to keep personal data confidential and secure and to protect it by following the Data Protection legislation and the Trust's policies. They are only permitted to process the data for the lawful purpose for which it has been shared and following the Trust's written instructions.

Data sharing in an emergency

We may also share personal data as is necessary and proportionate with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils and staff. An emergency includes, but is not limited to:

- preventing serious physical harm to a person
- preventing loss of human life
- protection of public health
- safeguarding vulnerable adults or children
- responding to any other emergency.

Data sharing as a legal obligation

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including:

- for the prevention or detection of crime and/or fraud
- for 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 its safeguarding obligations
- where there is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- where we need to liaise with other agencies – we will seek consent as necessary before doing this

Transferring personal data out of the UK

The Trust may, from time to time, transfer ('transfer' includes making available remotely), personal data to countries outside of the UK.

The transfer of personal data to a country outside of the UK shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the Secretary of State has determined ensures an adequate level of protection for personal data
- The transfer is to a country (or international organisation) that provides appropriate safeguards under Article 46 (2) of the UK GDPR
- The transfer is made under exceptional circumstances and one of the derogations in Article 49 of the UK GDPR applies including where the transfer is:
    - made with the informed consent of the relevant data subject(s)
    - is necessary for the performance of a contract between the data subject and the Trust(or for pre-contractual steps taken at the request of the data subject)
    - is necessary for important public interest reasons
    - is necessary for the conduct of legal claims
    - is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

- is made from a register that, under UK law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who can demonstrate a legitimate interest in accessing the register.

Individuals Rights

The Trust shall comply with Articles 13 – 23 of the GDPR which outline the rights of individuals under the regulation including:

- The right to be informed
- The right of access
- The right to rectification
- The right of erasure, in certain circumstances
- The right to restrict processing, in certain circumstances
- The right to data portability
- The right to object to processing in certain circumstances

The Trust shall respond to data subject rights requests without undue delay and within a calendar month of receipt of the request
That period may be extended by two months where necessary, taking into account the complexity and number of requests. The data subject will be informed of any extension within one month of receipt of the request, together with the reason for the delay.
See the Trust's *Individual Rights Policy and Procedure* for further information

Parental Requests to see the Educational Board

The parental right to access the pupil's educational record under section 5 (1) of The Education (Pupil Information) (England) Regulations (2005) does not apply to Academy Trusts. All parental requests to access a pupil's data beyond their statutory entitlement should be treated as a Subject Access Request and managed under the *Individual Rights Policy and Procedure*

CCTV

The Trust uses CCTV in various locations around the site to ensure the safety and security of individuals and property.

We will adhere to the Surveillance Camera Commissioner's Code of Practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Access to CCTV images is strictly controlled and recorded accordingly.

Any enquiries about the CCTV system should be directed to Mr Lee Warren IT Manager

For further information and guidance please refer to the Trust's *CCTV Policy and Viewing Procedure*

Privacy by Design and Default

The Trust will follow the UK GDPR by adopting a privacy by design and default approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into its processing activities.
We have a procedure to assess the processing of personal data perceived to be high risk, which may require a Data Protection Impact Assessment (DPIA) to be carried out, and processes to assist staff in ensuring compliance and privacy by design are an integral part of any processing we undertake.
For further information and guidance please refer to the Trust's *Data Protection by Design and Default Policy*

Accountability and Record Keeping

The Trust shall keep written internal Records of Processing Activities (RoPA), which shall incorporate the following information proscribed by Article 30 UK GPDR:

- The name and details of the Trust, the Trust's representative, the Data Protection Officer, and any applicable third-party processors
- The purposes of the processing
- Details of the categories of personal data collected, held and processed, and the categories of data subject to whom that personal data relates
- Details of any transfers of personal data outside the UK, including all mechanisms and security safeguards
- Details of how long personal data will be retained
- Detailed descriptions of all technical and organisational measures taken by the Trust to ensure the security of personal data.

Personal Data Breaches

A 'personal data breach' occurs when the confidentiality, integrity and/or availability of personal data is compromised. Personal data does not need to be stolen to be breached, it might also have been destroyed lost, altered, or disclosed to or accessed by unauthorised recipients.

The Trust has put in place procedures to deal with any suspected personal data protection breach and will notify data subjects or any applicable regulator where we are legally required to do so.

Data Protection Impact Assessments (DPIAs)

The Trust conducts DPIAs for all new, or changes to existing, technologies, programmes or third-party processing activities likely to result in a high risk to the rights and freedoms of data subjects,

Indicators of high-risk processing relevant to the Trust include, but are not limited to:

- the use of CCTV
- processing data concerning vulnerable data subjects (pupils)

DPIAs will be used to identify the most effective method of complying with the Trust's data protection

obligations and meeting individuals' expectations of privacy. Allowing the Trust to identify and resolve privacy issues at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation which might otherwise occur.

Data Security

Taking into account the state of the art, the cost of implementation, the nature, scope, context and purpose of the processing and the risks to the rights and freedoms of the individuals to whom the data relates, the Trust will use appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

- The pseudonymisation and/or encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to quickly restore availability and access to personal data in the event of a physical or technological incident
- A process for regularly testing assessing and evaluating the effectiveness of technological and operational measures for ensuring the security of the processing.

The Trust will also take steps to ensure that staff who have authorised access to personal data do not process the data except when carrying out their role and on instruction from the Trust

Training

All Trust staff and governors are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

Monitoring

The DPO and the Head of School are responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated as necessary in response to changes in the regulatory environment, where necessary in response to a serious data breach or data security incident, or otherwise every 2 years.

At each review, the policy will be shared with the full governing board.

Links with other Policies, Procedures and Records

This Data Protection Policy is linked to the Trust's:

- Appropriate Policy Document (see Appendix 1)
- Stakeholder Privacy Notices
- Individual Rights Policy and Procedure
- Information Security Policy
- CCTV Policy
- Data Breach Policy

- Records Management Retention Schedule & Policy
- Record of Processing Activities (RoPA)
- Freedom of Information policy
- Social Media Policy

Data Protection Policy: Staff Declaration

I confirm that:

- I have read and understood the Data Protection Policy
- I agree to abide by its terms
- I understand that any breach of Policy may result in disciplinary action

Name: _____

Signature: _____

Date: _____

Appendix 1: Appropriate Policy Document

For use when relying on specified conditions for the processing of special categories of personal data, and personal data relating to criminal convictions and offences

Introduction

This is the 'Appropriate Policy Document' required when Zest Academy Trust seeks to rely on any of the conditions specified in Schedule 1 to the Data Protection Act 2018, for the processing of special category and criminal convictions personal data.

The content of this Appropriate Policy Document meets the requirements of paragraph 39 of Schedule 1 of the Data Protection Act (2018), in that it –

- explains the Trust's procedures for securing compliance with the principles in Article 5 of the UK General Data Protection Regulation ('UK GDPR') - relating to the processing of personal data, in connection with the processing of personal data in reliance on the condition in question; and
- explains the Trust's policies as regards the retention and erasure of personal data processed in reliance on the condition, indicating how long such personal data is likely to be retained.

Under paragraph 40(1) of Schedule 1 of the DPA (2018), where the Trust processes personal data in reliance on a condition described in paragraph 38 of Schedule 1, they will, during the relevant period[1]:

- retain the appropriate policy document,
- review and (if appropriate) update it from time to time, and
- make it available to the Information Commissioner, on request, without charge

Description of Data Processes

As part of its statutory and business functions, the Trust processes special category data related to stakeholders, including staff, Trustees/Governors and volunteers, staff, job applicants, pupils and parents/carers.

This includes where relevant, information about health, disability and wellbeing, ethnicity, trade union membership, religious or philosophical beliefs, and biometric data. Further information about this processing can be found in the relevant stakeholder ***Privacy Notices***.

Processing for reasons of substantial public interest relates to the data the Trust receives, obtains, or creates to fulfil our statutory obligations. For example, this may be related to the safeguarding of pupils, supporting staff with a particular disability or medical condition, equal opportunities monitoring, safeguarding, etc. A record of our processing activities is kept under Article 30 of the UK GDPR.

[1] *The 'relevant period' begins when the data is collected and ends no less than 6 months following cessation of the processing*

Schedule for Processing

The Trust processes special category data for the following purposes in Part 1 of Schedule 1 of the Data Protection Act (2018):

- Paragraph 1: Employment, social security and social protection.

The Trust may process special category data for the following purposes in Part 2 of Schedule 1 of the Data Protection Act (2018):

- Paragraph 6: Statutory, etc. purposes.
- Paragraph 8: Equality of opportunity and treatment.
- Paragraph 16: Support for individuals with a particular disability or medical condition
- Paragraph 17: Counselling
- Paragraph 18: Safeguarding of children and individuals at risk
- Paragraph 20: Insurance
- Paragraph 21: Occupational Pensions

Criminal Offence Data
The Trust processes criminal offence data for the following purposes in parts 1 and 2 of Schedule 1 of the Data Protection Act (2018).

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes
- Paragraph 18 (1) Safeguarding of Children and individuals at risk

Securing Compliance with the Data Protection Principles

The Trust's procedures for complying with Article 5 of the GDPR: Data Protection Principles are as follows:

Principle A: Personal data shall be processed lawfully, fairly and in a transparent manner.
The Trust will:

- ensure that personal data is only processed where at least one of the conditions in Schedule 1 is met or the data subject has given explicit consent for the processing.
- only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing.
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent (provision of privacy notices).
- where necessary carry out Data Protection Impact Assessments to ensure proposed processing is carried out fairly.

Principle B: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
The Trust will:

- only collect personal data for specified, explicit and legitimate purposes and will inform data subjects what those purposes are through the provision of privacy notices.
- not use personal data for purposes that are incompatible with the purposes for which it was collected.
- before personal data is used for a new purpose that is compatible, the Trust will inform the data subject.

Principle C: Personal data shall be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
The Trust will:

- only collect the minimum personal data needed for the purpose for which it is collected.
- ensure the data is adequate and relevant to the purpose for which it is collected.
- apply Data Protection Impact Assessments to ensure the proposed processing is not excessive.
- Where personal data is provided to, or obtained by the Trust but is not relevant to a stated purpose, it will be erased.

Principle D: Personal data shall be accurate and, where necessary, kept up to date.
The Trust will ensure that:

- personal data is accurate and kept up to date as necessary.
- when notified of inaccuracies personal data is corrected.
- where the Trust become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, every reasonable step will be taken to ensure that data is erased or rectified without delay. If the Trust decides not to either erase or rectify it, for example, because the lawful basis relied upon to process the data means these rights don't apply, the decision not to erase will be documented.

Principle E: Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
The Trust will ensure that:

- personal data will only be kept in identifiable form only as long as is necessary for the purposes for which it is collected unless otherwise required by law.
- when no longer needed, personal data shall be securely deleted or anonymised.
- personal data is held and disposed of in line with the Trust's Data Retention Policy and Schedule.

Principle F: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.
The Trust will ensure that:

- there are appropriate organisational and technical measures in place to protect personal data.

- data is processed following all relevant data protection policies and procedures.

The Accountability Principle

Under the UK GDPR Article 5(2), the Trust is responsible for and must be able to demonstrate compliance with the principles listed above.

The Trust has appointed a Data Protection Officer. The DPO provides independent advice and monitoring of personal data handling and has access to report to the highest management level.

The Trust will:

- ensure that records are kept of all personal data processing activities and that these are provided to the Information Commissioner on request (RoPA).
- carry out a Data Protection Impact Assessment for any high-risk personal data processing and consult the Information Commissioner if appropriate.
- have in place internal policies and procedures to ensure that personal data is collected, used or handled only in a way that is compliant with data protection law.
- Maintain a Policy and Schedule for the retention and erasure of Personal Data

The Trust will ensure, where special category or criminal convictions personal data is processed, that:

- there is a Record of Processing Activities (ROPA), and that record will set out, where possible, the envisaged time limits for the erasure of the different categories of data.
- where special category or criminal convictions personal data is no longer required for the purpose for which it was collected, it will be securely deleted or rendered permanently anonymous following the Trust's Data Retention Policy and Schedule.
- data subjects receive a Privacy Notice (sometimes called a fair processing notice) detailing how their data will be handled, including the period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period.

Additional Special Category Processing

The Trust processes special category personal data in other instances where there is no requirement to keep an Appropriate Policy Document. Our processing of such data is in accordance with data protection legislation and respects the rights and freedoms of the data subjects.

The Trust will provide clear and transparent information about why personal data is processed including the lawful basis for processing in stakeholder Privacy Notices. Copies of Privacy Notices are available from the office.