PENK VALLEY ACADEMY TRUST

General Data Protection Regulation Policy

Adopted by Trustees:	
Signed:	
Date:	Spring 2026
This policy is reviewed annually by the Audit Finance and Risk Committee	
Next Review date:	Spring 2027

COLLABORATION CHALLENGE CURIOSITY CARE

POLICY INFORMATION

Date of last review:	Spring 2026	**Review period:**	Annually
Date ratified by Trustees:	Spring 2026	**Trustee committee responsible:**	Audit Finance and Risk
Policy owner:	Chief Operations Officer	**Executive team member responsible:**	Chief Operations Officer

Reviews/revisions

Review date	Changes made	By whom
March 2023	New policy.	LMC
January 2024	Updates to DPO and DPL	LMC
March 2025	No changes	LMC
March 2026	Full rewrite in line with Schools DPO model policy	LMC

Equality and GDPR

All Penk Valley Academy Trust policies should be read in conjunction with our Equal Opportunities and GDPR policies.

Statement of principle – Equality

We will take all possible steps to ensure that this policy does not discriminate, either directly or indirectly against any individual or group of individuals. When compiling, monitoring and reviewing the policy we will consider the likely impact on the promotion of all aspects of equality as described in the Equality Act 2010.

Statement of principle – GDPR

Penk Valley Academy Trust recognises the serious issues that can occur as a consequence in failing to protect an individual adult's or child's personal and sensitive data. These include emotional distress, physical safety, child protection, loss of assets, fraud and other criminal acts.

Penk Valley Academy Trust is therefore committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA)/GDPR.

Penk Valley Academy Trust will be referred to as **PVAT** for the remainder of the document which includes all schools who are members of PVAT, business operations and centralised services.

GENERAL DATA PROTECTION REGULATION POLICY

Contents

Contents ..... **Error! Bookmark not defined.**
1.Policy Statement 4
2.Legislation 4
3. Contact 4
4. Roles and Responsibilities 4
3.1 All Staff 5
4.Data Protection Principles 5
5. Lawfulness, fairness and transparency 6
5.1 Lawfulness 6
5.2. Criminal Convictions and Offences 7
5.3. Fairness and transparency 7
6. Purpose limitation 8
7. Data minimisation 8
8. Accuracy 8
9. Storage limitation 8
10. Security 9
11. Accountability 9
12. Data Protection Impact Assessments 10
13. Sharing Personal Data 10
14. Subject Access Requests 11
14.1. Children and Subject Access Requests 11
14.2.Responding to Subject Access Requests 12
15. Other Data Protection Rights of the Individual 12
16. CCTV 13
17. Biometric Recognition Systems 13
18. Photos and Videos 14
18. Generative Artificial Intelligence (AI) 14
19. Personal Data Breaches 15
19.1. Data Breach Register 15
19.2. Data Breach Response Plan 15
20. Training 15
21. Concerns and Complaints 15
22. Monitoring Arrangements 18
23. Links with Other Policies and Procedures 18
24. Appendix One - Definitions 18

1.Policy Statement

We need to collect and use personal information so that we can operate effectively as a school and fulfil our statutory duties. The information we collect and use includes information about pupils, parents, employees, governors, suppliers, visitors etc.

We are committed to protecting the privacy and security of this personal information at all times, and supporting individuals in exercising their rights in relation to their own personal information.

This policy, along with accompanying procedures and associated policies, sets out our commitment and approach to safe data protection practice, as well as our support for individuals in exercising their rights. It applies to all personal data, regardless of whether it is in paper or electronic format.

It is reviewed annually and updated in line with any changes to data protection legislation.

2.Legislation

This policy meets the requirements of the UK General Data Protection Regulation (GDPR) and the provisions of the UK's Data Protection Act 2018.

Under the GDPR our school is classified as a Data Controller and we are registered with the UK's supervisory authority, the Information Commissioner's Office (ICO). Our registration is renewed annually.

3. Contact

If you would like to discuss anything in this policy, please contact our Headteacher or Data Protection Officer (DPO) as follows:
Headteacher -
DPO - Nicola Cook, SchoolsDPO, nicola@schoolsdpo.com

4. Roles and Responsibilities

This policy applies to all staff employed by our school, as well as to external organisations or individuals working on our site.

Staff who do not comply with this policy may face disciplinary action, which could include dismissal. It is a criminal offence to access personal data held by the school for other than school business, or to procure the disclosure of personal data to a third party, or to sell such data.

PVAT has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

The Headteacher has the responsibility for ensuring the implementation of this policy within their individual setting. They 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.

The Data Protection Officer monitors compliance with data protection law, providing support and guidance as required.

3.1 All Staff

All Staff are responsible for ensuring that they process any personal data in accordance with this policy (a definition of processing can be found in Appendix 1). Staff must also inform the office of any changes to their personal data, such as a change of address.

Staff must contact the office whenever they have a query about data protection, including, but not limited to the following:

any questions about the operation of this policy: including retaining personal data; keeping personal data secure; sharing personal data with third parties; or whether there is a lawful basis in place for a particular data processing operation

- Any concerns that the policy is not being followed
- A new project under consideration that involves the processing of personal data
- Received any requests from individuals for access to their personal information the school is processing.

4.Data Protection Principles

The UK GDPR sets out seven key principles which form the foundation of this data protection legislation:

1. Lawfulness, fairness and transparency - Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals

2. Purpose limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

3. Data minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. Accuracy - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

5. Storage limitation - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes. This is subject to implementation of the appropriate technical and organisational measures required by the GDPR, in order to safeguard the rights and freedoms of individuals

6. Integrity and confidentiality (security) - 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

7. Accountability - the controller shall be responsible for, and able to demonstrate, accountability with the GDPR principles.

This Data Protection Policy, along with our privacy notices and additional policies and procedures referenced in section 25, sets out how our school aims to comply with these principles.

5. Lawfulness, fairness and transparency

5.1 Lawfulness

We will always ensure we have a valid lawful basis for our processing of personal data. There are six lawful bases we can rely on under the UK GDPR:

1. Contract - the processing is necessary for a contract with an individual, or because they have asked for specific steps to be taken before entering into a contract.

2. Legal obligation - the processing is necessary to comply with the law (not including contractual obligations).

3. Vital interest - the processing is necessary to protect someone's life.

4. Public task - the processing is necessary to perform a task in the public interest or for our official functions as a school, and the task or function has a clear basis in law.

5. Legitimate interests - the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

6. Consent - the individual has given clear and informed consent for their personal data to be processed for a specific purpose. The individual can change their mind at any time and withdraw their consent. If this happens the processing will be stopped.

Some personal data is considered more sensitive under the GDPR, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information (such as fingerprints, retina and iris patterns), where used for identification purposes, health – physical or mental, sex life or sexual orientation.

For these special categories of personal data, we will also identify one of the special category conditions for processing set out in the GDPR:

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies

- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law).

In addition, under the UK's Data Protection Act 2018, we rely on the processing conditions at Schedule 1 part 1, paragraphs 1, 8 and 18. These relate to the processing of special category data for employment purposes, safeguarding and equality of opportunity/treatment.

Our Appropriate Policy Document provides more information about this processing on PVAT's website. www.penkvalley.co.uk/

5.2. Criminal Convictions and Offences

The UK GDPR also gives extra protection to criminal offence data. As well as ensuring a valid lawful basis for the processing of criminal offence data under the GDPR, we will also identify an additional condition set out in Schedule 1 of the UK DPA 2018.

Under Article 6 of the GDPR, lawful bases we rely to process this data are:

- Performance of our public task
- Performance of a contract.

In addition, under the UK's Data Protection Act 2018, we rely on the processing conditions at Schedule 1:

- Part 2, para 6(2)(a)
- Part 1, para 1.

These relate to the processing of criminal offence data for statutory and employment purposes respectively. See Part 3 of Keeping Children Safe in Education for more information.

Our Appropriate Policy Document provides more information about this processing.

5.3. Fairness and transparency

Data protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by the GDPR.

This will normally be through our privacy notices:

- Our Privacy notice for Pupils and Parents / Carers sets out how we process pupil personal data to support teaching and learning, to provide pastoral care and to assess the performance of our services.

- Our Privacy Notice for Employees, Workers and Contractors sets out how we process the personal data of staff, agency staff and contractors to fulfil our obligations as an employer.

- Our Privacy Notice for Governors sets how we process governors' personal data to support them in fulfilling their governance role.

- Our Privacy Notice for Job applicants sets how we process job application data to support the selection and recruitment of staff.

All our Privacy Notices also include information on the rights of the individuals whose data we are processing and who to contact to discuss any aspect further.

6. Purpose limitation

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to individuals when we first collect their data (usually through our privacy notices).
If we need to use personal data for reasons other than those given when we first obtained it, we will identify and document a new lawful basis; although this may not be necessary if our new purpose is compatible with the original purpose. We will inform the individuals concerned before we do so, and seek consent where necessary.

7. Data minimisation

We will only collect the minimum amount of personal data necessary for our purposes. Staff will only process personal data where it is necessary to perform their roles.

8. Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs us of a change of circumstances, their records will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, we will immediately mark the record as potentially inaccurate, or "challenged".

9. Storage limitation

When our school no longer needs the personal data it is processing, it will be deleted or anonymised. This will be done in accordance with our data retention schedule.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use an outside company to convert paper records to electronic files and shred documents on site.

Where details of individuals are stored for long-term archive, historical or statistical reasons, this will be done within the requirements of the GDPR.

10. Security

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

All members of staff are required to sign to confirm that they have read and understood this Data Protection Policy.

All members of staff are required to sign an acceptable user agreement which is renewed annually. The acceptable user agreement is linked to the school's ICT Security Policy and covers such aspects as:

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information being kept securely when not in use
- Papers containing personal information being kept secure and not being left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- Staff ensuring that individual monitors do not show confidential information to passers-by and that they log off from their device when it is left unattended
- Staff adhering to school policies and procedures when taking data off site and when working remotely or at home
- Strong passwords being used to access school systems, online resources, laptops and other electronic devices. These must be at least 8 characters long containing letters and numbers; or preferably passphrases (e.g. 3 unconnected words).
- Encryption software being used to protect all portable devices and removable media
- Staff not storing personal information on their personal devices and being expected to follow the same security procedures as set out for any school owned equipment
- GDPR compliant cloud storage being used for all online data storage
- The use of USB devices not being allowed to store personal data.

11. Accountability

The school has put in place appropriate technical and organisational measures to meet the requirements of the accountability principle These include:

- The appointment of a data protection officer who reports directly to our highest management level
- Taking a 'data protection by design and default' approach to our activities
- Maintaining accurate documentation of our processing activities, such as the purposes of processing personal data, data sharing and retention. We also document the lawful bases and conditions we are relying on for our purposes, including how and when consent was obtained, as appropriate
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our high risk processing (see section 6).

We regularly review our accountability measures and update or amend them when required.

12. Data Protection Impact Assessments

The GDPR requires us to carry out Data Protection Impact Assessments (DPIAs) for any type of processing that is likely to result in a high risk to individuals' interests; for example, when introducing new technologies, or using biometric data for identification purposes.

To assess the level of risk, we consider both the likelihood and the severity of any impact on individuals. High risk can result from either a high probability of some harm, or a lower possibility of serious harm.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

As part of our data protection by design and default approach we will carry out a DPIA for any other major project which requires the processing of personal data.

We follow the ICO's guidelines and our DPIAs:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks.

13. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

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

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

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

Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with the international transfer rules in the GDPR .

Where we share personal data on an ad hoc or 'one off' basis, we will record the details including our purpose and lawful basis for doing so.

14. Subject Access Requests

Under the GDPR, anyone whose personal data we are processing, e.g staff, pupils and parents\carers etc, has a right to make a 'subject access request' to gain access to information our school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests can be made by contacting any member of staff, but it is helpful if they are made to the School Office or the DPO. They can be made in person, verbally, in writing, and by email. The following information will be required:

- Name of individual
- Relationship of the requester to the individual, if appropriate
- Correspondence address
- Contact number and email address
- Details about the information requested

Completion of a subject access request form can be useful, but this cannot be insisted upon.

If a member of staff receives a subject access request they must immediately forward it to the School Office.

Members of staff can find further information on their role in handling subject access requests in our Guidance for Staff.

14.1. Children and Subject Access Requests

A child's personal data always belongs to them rather than the child's parents or carers.
For a parent or carer to make a subject access request, with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

The UK's Information Commissioner's Office generally regards children aged 12 and above to be mature enough to understand their rights and the implications of a subject access request. However, we will always consider this on a case by case basis.

14.2. Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification, if necessary
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not reveal the following information in response to Subject Access Requests:

- Information that might cause serious harm to the physical or mental health of the subject or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child
- Any references that have been provided or received in confidence.

If the request is considered unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be considered to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

15. Other Data Protection Rights of the Individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it (see section 6), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the United Kingdom
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO

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

If staff receive such a request, they must immediately forward it to the school office.

16. CCTV

Where our schools use CCTV to enhance site security. Cameras are positioned in various locations. They are clearly visible and accompanied by prominent signs explaining CCTV is in use. Further information on our use of CCTV is set out in our CCTV Policy and any queries should be directed to the office.

17. Biometric Recognition Systems

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person. This can include a person's fingerprints, facial shape, retina and iris patterns and hand measurements. All biometric data is considered special category data under the GDPR.

Where we use biometric data we will ensure that it is treated with appropriate care and that we comply with the GDPR principles.

Where biometric data is used as part of an automated biometric recognition system, e.g. cashless catering or photo ID card systems, we will comply with the additional requirements of the Protection of Freedoms Act 2012 (sections 26 - 28). The school will:

- Ensure that each parent is notified of the school's intention to use their child's biometric data as part of an automated biometric recognition system
- Ensure consent of at least one parent is obtained for all pupils under the age of 18 before the data is taken from the pupil and used
- Not process the biometric data of a pupil (under the age of 18) where:
    - the pupil objects or refuses to participate in the processing of their biometric data (their objection or refusal can be verbal, it does not have to be in writing)
    - no parent has consented to the processing (this must be a written consent, and can be though a digital form collection)
    - a parent has objected in writing even if another parent has given their consent.

Parents and pupils can change their minds and withdraw consent at any time. We will make sure that any biometric data already captured is deleted.

We will provide alternative means of accessing services for those pupils who are not using an automated biometric system.

When notifying parents about the intention to take and use their child's biometric information as part of an automated biometric system, we will include:

- Details about the type of biometric data to be taken
- How it will be used
- The parents' and pupil's right to refuse or withdraw their consent at any time
- Our duty to provide reasonable alternative arrangements for those pupils who will not be using the automated biometric system.

**'parents' includes not only the biological mother or father (or the adoptive parents) but any individual with parental responsibility for the child, as set out in Part 1 of the Children Act 1989.*

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object or withdraw their consent. Consent can be withdrawn at any time and any biometric data already held will be deleted.

18. Photos and Videos

As part of our educational activities, we may take photographs and record images of individuals. We will always clearly explain to pupils and/or parents (as appropriate) how the photograph or video will be used.

We will obtain consent for photographs and videos to be taken of pupils for marketing and promotional materials.

Uses may include:

- In school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media page.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the individual, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

18. Generative Artificial Intelligence (AI)

A separate policy for Ai is available and covers the aspects of GDPR .
AI models in use within the trust are assessed and implemented with GDPR at its core.

19. Personal Data Breaches

The GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

When a personal data breach has occurred we will assess the likelihood and severity of the resulting risk to the rights and freedoms of the individuals involved. If it's likely that there will be a risk, then we are required by law to notify the ICO.

19.1. Data Breach Register

We record all breaches of personal data, regardless of whether they are reported to the ICO. Our data breach register includes the details of the breach, its effects and any remedial action taken. Remedial action may include a review of relevant systems or policies and procedures; additional training for staff; or other corrective steps, as appropriate.

19.2. Data Breach Response Plan

Each breach will be considered on a case by case basis but will broadly follow our Data Breach Response Plan

If any member of staff believes a breach of personal data has occurred, or might have occurred, they are required to let the headteacher know immediately.

20. Training

Our staff are provided with data protection training as part of their induction process and this is refreshed at least annually. We take a blended approach, so training may be formal CPD - face to face or online delivery; through INSET days, staff meeting updates and discussion, 1:1 reviews, newsletters etc.

Uptake of training is monitored and procedures are in place to ensure that all staff complete the required training.

21. Data Protection Complaints

We will always endeavour to resolve any concerns about our processing of personal data informally where possible.

However, individuals have the right to make a formal data protection complaint under the UK Data (Use and Access) Act 2025. This is a separate statutory process from the school's general complaints procedure.

How to make a complaint
To help us investigate your concern quickly and efficiently, complaints should be submitted using the Trust's online Data Protection Complaint Form:
Data Protection Complaint Form – Fill in form

The form is designed to ensure that all information necessary to investigate the complaint is provided at the outset.

Complaints may also be submitted by:

- Email
- Letter
- Telephone
- In person

The Trust will not refuse to accept a complaint because the online form has not been used. Where insufficient information has been provided to understand or investigate the complaint, the Trust will contact the complainant **without undue delay** to request clarification or additional information.
Data protection enquiries may be directed to: **enquiries@penkvalley.co.uk**

Receipt and Recording of Complaints
A complaint is received on the date it reaches the Trust. This includes complaints submitted electronically outside normal working hours, during school holidays or during periods of school closure.

All data protection complaints will be recorded without undue delay. The date on which a member of staff first opens or reads a complaint does not change its date of receipt.

Recording receipt of a complaint does not necessarily mean that it has been reviewed, allocated for investigation or formally acknowledged.

Where the Trust sends an automatic message confirming that a form or email has been received, this confirms receipt only and does not constitute formal acknowledgement unless the message specifically states that it is the Trust's formal acknowledgement.

The availability of the staff needed to review or investigate a complaint may be affected by school holidays, periods of closure, staff leave or public holidays. This may affect when particular enquiries can be undertaken, but the Trust will continue to progress the complaint without undue delay, taking account of the circumstances and the availability of the relevant staff.

School holidays and periods of closure do not change the date on which a complaint is received or affect the complainant's statutory rights.

Acknowledgement
The Trust will formally acknowledge all data protection complaints within 30 calendar days of receipt.

The 30-day period begins on the day after the complaint is received. If the final day falls on a weekend or public holiday, the formal acknowledgement will be provided on the next working day.
The Trust will normally seek to provide formal acknowledgement sooner than the maximum statutory period.

The formal acknowledgement will normally:

- confirm the date on which the complaint was received;
- confirm that the complaint has been recorded;
- confirm that the Trust will investigate the matters raised;
- provide a point of contact for enquiries;
- explain what will happen next; and
- provide an indication of the expected timescale, where possible.

Where an electronic or automatic response specifically states that it is the Trust's formal acknowledgement, no separate acknowledgement will be required.
An automated message that only confirms successful submission or receipt will not constitute formal acknowledgement.

The 30-calendar-day period applies only to formal acknowledgement. It is not the deadline for the investigation or the outcome.

Investigation
The Trust will take appropriate steps to investigate the complaint without undue delay.

The investigation will be appropriate and proportionate to the nature, complexity, seriousness and circumstances of the complaint. It will not be delayed solely because the formal acknowledgement has not yet been issued.

Where a complaint is received during a school holiday or period of closure, the Trust will take any steps that are reasonably available. Some enquiries may need to wait until the relevant staff return or the necessary records become available. Once they are available, the investigation will be progressed without undue delay.

During the investigation, the Trust may:

- review relevant records, correspondence and systems;
- seek clarification or further information from the complainant;
- consult relevant members of staff;
- obtain information from third parties, where appropriate and lawful; and
- obtain advice from the Trust's Data Protection Officer or other professional advisers.

Keeping you informed
The Trust will keep complainants appropriately informed throughout the process and will:

- Provide an estimated timescale where possible.
- Notify complainants of any significant delays.
- Provide a contact point for enquiries regarding the complaint.
- Request further information where necessary to complete the investigation.

Outcome
The Trust will communicate the outcome of its investigation without undue delay.

The response will normally include:

- A summary of the complaint investigated.
- The findings of the investigation.
- Any actions taken or proposed by the Trust.
- Information about further rights of complaint.

Right to complain to the ICO
The Trust encourages individuals to raise concerns directly with the Trust in the first instance so that matters can be investigated and, where appropriate, resolved promptly.

If an individual remains dissatisfied with the outcome of the Trust's investigation, or believes their data protection rights have been infringed, they may complain to the Information Commissioner's Office (ICO).

Website: www.ico.org.uk
Telephone: 0303 123 1113

22. Monitoring Arrangements

The Finance Audit and risk committee is responsible for monitoring and reviewing this policy. It will be reviewed on an annual basis.

23. Links with Other Policies and Procedures

This Data Protection Policy is linked to:

AI Policy
Appropriate Policy Document
BYOD
CCTV Policy
Data Breach Response Plan
Online Safety
Cyber security and Acceptable use
Freedom of Information Publication Scheme.
Guidance for Staff on Subject Access Requests
Privacy Notice for Pupils and parents, Carers
Privacy Notice Employees workers and contractors
Privacy Notice for Governors
Privacy Notice for Job Applicants
Record Retention Schedule
Safeguarding Policy

24. Appendix One - Definitions

Personal data - Data from which a person can be identified (i.e. distinguished from other individuals); such as:

- Name (including initials)

- Identification number
- Location data
- email address, telephone number, car registration number
- Online identifier, such as a username, IP addresses, cookie identifiers
- photographs, video recordings

This includes data that, when combined with other readily available information, leads to a person being identified.

Special category
persona data Personal data which is more sensitive and is therefore afforded more protection under the GDPR.

Data such as:

- Racial or ethnic origin
- Political opinions
- Religious beliefs, or philosophical beliefs
- Where a person is a member of a trade union
- genetic data
- biometric data (when used for identification purposes)
- Physical and mental health
- Sexual orientation and sex life

Data relating to criminal convictions is afforded similar special protection.

Processing
Any operation carried out on personal data, such as
collecting, recording, storing, altering, retrieving, using,
disseminating, erasing or destroying.

Processing can be automated or manual.

Data subject - The living individual whose personal data is held or processed.

Data controller - A person, or organisation, that determines the purpose for which, and the way, personal data is processed.

Data processor - A person, or other body, other than an employee of the data controller, who processes the data on behalf of the data
controller.

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

Breaches can be the result of accidental or deliberate causes.