Warrington Primary Academy Trust

Data Protection Policy V7

Ratified:1 April 2025

Next Review Date: April 26

Policy Responsibilities and Review

Policy type:	Trust Wide
Guidance:	This policy uses guidance from: • Working Together to Safeguard Children 2018 • KCSIE • Data Protection Act 2018 • UK General Data Protection Regulations (UK GDPR) • Protection of Freedoms Act 2012
Related policies:	• Information Management • Acceptable Use Protocols • Safeguarding Policy • Special Category Data Policy
Review frequency:	Annually
Committee responsible:	Resources Committee
Chair of Trustees signature:	
Changes in latest version:	V7 Nov 2025: Pg.6: 5.2. Changed person responsible

Contents

1. Aims 4
2. Legislation and guidance 4
3. Definitions 5
4. The data controller 6
5. Roles and responsibilities 6
6. Data protection principles 7
7. Collecting personal data 7
8. Sharing personal data 9
9. Subject access requests and other rights of individuals 9
10. Parental requests to see the educational record 11
11. Biometric recognition systems 11
12. CCTV 12
13. Photographs and videos 12
14. Data protection by design and default 13
15. Data security and storage of records 13
16. Disposal of records 14
17. Personal data breaches 14
18. Training 14
19. Monitoring arrangements 14
Appendix 1: Personal data breach procedure 15
Appendix 2: Information Management and Acceptable Use Protocol 19

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulations and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the DPA 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 subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 in terms of any future use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Schools that use CCTV:
Beamont
Evelyn Street
Others TBA

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Biometric data • Health • Sex life • Sexual orientation • Trade union membership • Medical conditions
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.

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

4. The data controller

As well as the MAT, all schools within the Trust process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore are data controllers.

The MAT is registered as a data controller with the ICO, with all WPAT schools listed, and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trustees and Local Governing board

The Trustees and Local Governing Boards have overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

5.2 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.

They will provide an annual report of their activities directly to the WPAT Board of Trustees and, where relevant, report to the board their advice and recommendations on school's data protection issues.

The DPO is also the first point of contact for individuals whose data the school's processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

The Trust DPO is Tru Digital and is contactable via the WPAT central office dpo@wpat.uk

5.3 Headteacher / Business Manager

The Headteacher and Business Manager act as the main point of contact for the data manager on a day-today basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Data Manager and 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 European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

The special categories of personal data that we collect and the reasons for collecting them are below:

Racial/ Ethnic Origin

Collected for pupils as part of the School Census

Collected for staff as part of the School Workforce Census

Trade union membership

Collected only for support staff and for those wishing to pay for membership through payroll

Medical conditions

Collected for staff and pupils to ensure their welfare and safety in school and for any medical emergencies that might occur.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a privacy notice or information within a consent form.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

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.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's document retention schedule, stored within shared files in the Trust M drive.

8. Sharing personal data

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

- An FOI request commits us. (See FOI statement from Information Commissioner's Office (ICO) on Trust Website.)
- 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 which 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 European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the 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 should include:

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

If staff receive a subject access request they must immediately report it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not 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.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- 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 disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is 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 deemed 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.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), 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 European Economic Area
- 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)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

There is no automatic parental right of access to the educational record in academies, however within WPAT schools we believe that parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within one month of receipt of a written request.

11. Biometric recognition systems

We currently do not collect any biometric data from our staff or children in our schools. The following section outlines policy should we introduce it in the future.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, if pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

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. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around some of our school sites to ensure they remain safe. We adhere to the ICO'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.

Any enquiries about the CCTV system should be directed to the school Headteacher or Business Manager

13. Photographs and videos

As part of our school's activities, we may take photographs and record images of individuals.

We will obtain written consent from parents/ carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/ carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/ carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school, on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school, by external agencies such as the school photographer, newspapers, campaigns
- Online, on our school/ Trust website or social media pages

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

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

See our child protection and safeguarding policy for more information on our use of photographs and videos.

14. Data protection by design and default

The Trust will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

WPAT schools and the Trust Central Service 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.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site in physical format, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who access personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Information Management policy and acceptable use pro forma.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- Two factor authentication is used on systems that have the most confidential data stored within them, i.e. our main MIS and safeguarding MIS.

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite, delete or archive electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The school will make all reasonable endeavors to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All 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 school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared widely across the Trust.

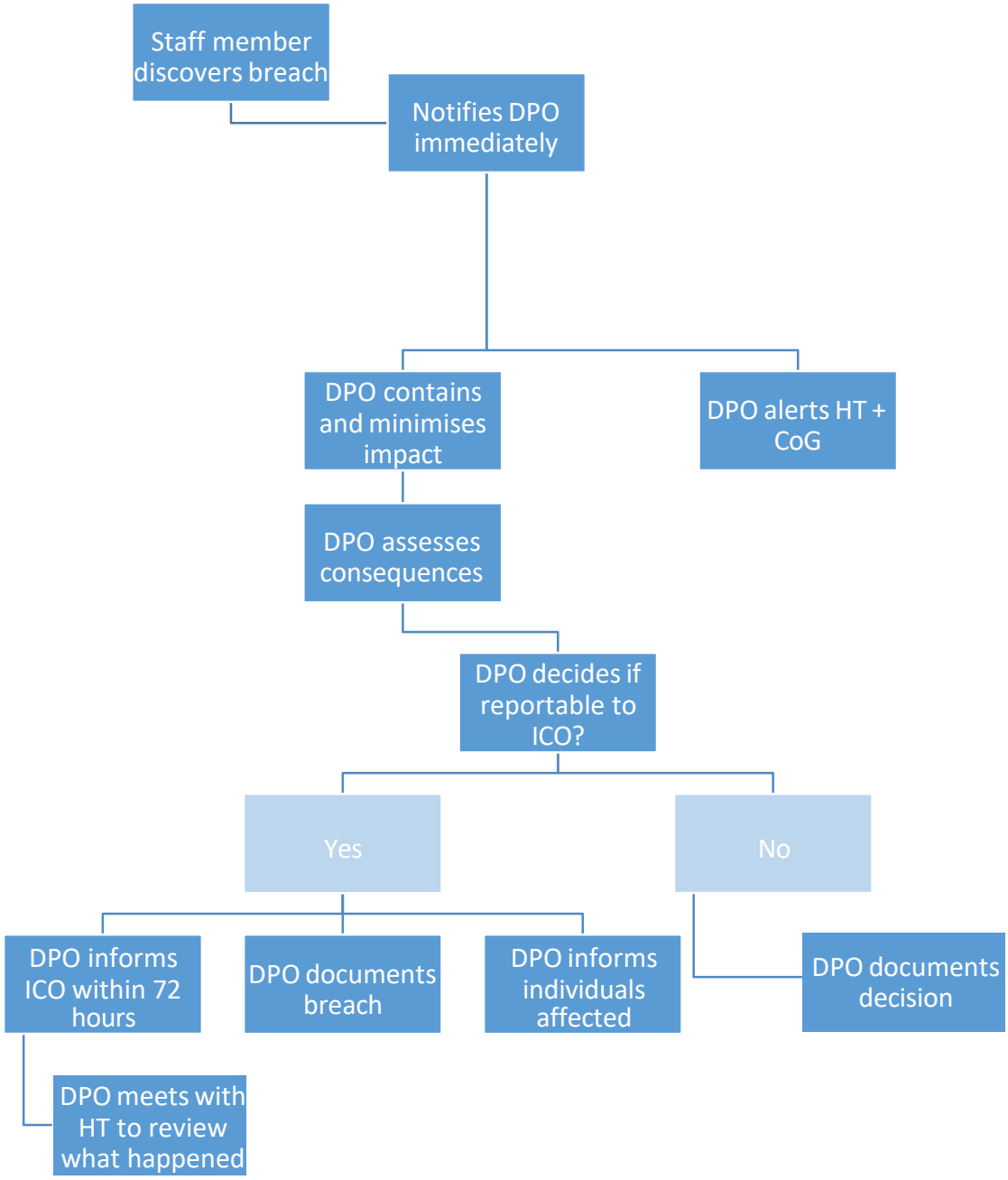
Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and in the case of a breach reportable to the ICO, the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g.
    - emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud o Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
    - If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the shared M drive with named limited access limited to the Headteacher and Business Manager of each school and Trust DPO.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on the Trust M drive with named limited access files.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The number of breaches, near misses and SAR's are reported termly to the Trust Board

The following diagram represents the process detailed above.



Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

• Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

• If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

• In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

• The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

• The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2: Information Management and Acceptable Use Protocol

To be used alongside Data Protection Policy

1. Purpose

This information management and acceptable use protocol provides clear direction and support for information security that is applicable to all staff at all levels of the organisation. The policy describes the means by which the school aims to preserve confidentiality, integrity and availability of data.

Confidentiality: information is accessible only to those authorised to have access

Integrity: safeguarding the accuracy and completeness of information

Availability: ensuring that authorised users have access to information when required.

It is acknowledged that the Trust and each of the schools within the Trust have legal, statutory and contractual requirements with which they must comply. The school complies with the rules of good information handling, known as the data protection principles, and the other requirements of GDPR (General Data Protection Regulations)

This policy will be reviewed annually and updated as necessary.

Specialist security advice will be sought where necessary. EDAC and Pennine will be consulted as a source of such advice, for example for data protection or network security issues.

2 Personnel security

2.1 Security responsibilities

Security responsibilities are clearly documented and, where appropriate, addressed at the recruitment phase and included in contracts of employment. Personnel screening processes for permanent and temporary staff include appropriate controls (e.g. availability of satisfactory references, confirmation of claimed academic and professional qualifications, independent identity checks). There is a formal disciplinary process for employees who violate security policies and procedures and employees are made aware of the action to be taken if they disregard security requirements.

2.2 Information security education and training

All staff receive appropriate training and regular updates in security policies and procedures before access to systems is granted. This includes training in security requirements, controls and legal requirements, as well as in the correct use of information systems (e.g. log-on procedures).

2.3 Responding to security incidents and malfunctions

In the event that a member of staff becomes aware of a security incident, malfunction or weakness, the Business Manager of the school must be informed immediately, who must contact the Data Protection Officer. Recovery is carried out only by appropriately trained and experienced staff. Users are made aware that they should not, under any circumstances, attempt to prove a suspected security weakness as this could be interpreted as potential misuse of the system and may be subject to disciplinary procedures.

2.4 Third party involvement

Any third party engaged by the Trust or the school from must sign and adhere to the data management agreement. No third party will install, update, or amend any device, network or system without the explicit and written agreement of the Headteacher or CEO of the Trust.

3 Physical and environmental security

3.1 Secure areas

Areas in which critical or sensitive information is processed are physically secured to prevent unauthorised access, damage or interference. Control is achieved by conventional security procedures (e.g. doors and windows locked when unattended, CCTV). Access to secure areas is controlled and restricted to authorised personnel only, with the use of keys which are removed from site at the end of each day.

3.2 Equipment security

Equipment is sited or protected to minimise the risk of theft and damage (e.g. fire, water, impact, power surge). Cabling is protected from interception or damage (e.g. use of conduit, fibre, avoidance of public areas). Equipment is correctly maintained and serviced by authorised personnel. Equipment is labelled and logged on the school asset register. Staff must share any concerns over the safety of equipment with the Business Manager of the school in the first instance.

3.3 Off-site security

Equipment is not taken off-site without authorisation. Equipment and media taken off the premises must not be left unattended outside of the home of that member of staff. Portable computers must be carried as hand luggage and disguised where possible when travelling. Home working is subject to suitable controls. When working at home, staff must ensure that all personal or sensitive information is kept out of sight from other family members or visitors. Use of WPAT equipment (e.g. laptops) is prohibited by non-WPAT staff. Where staff have the facility of remote access, secure and complex passwords must be used for connection.

3.4 Mobile technology

Accessing WPAT emails on personal devices is limited to those with InTune installed, and emails must be accessed exclusively through WPAT-approved apps within InTune. This ensures documents cannot be downloaded or saved on personal devices and introduces additional security measures for email access.

3.5 Movement of information

Within school, all personal or sensitive information must be stored on the WPAT network. Access to this network is available throughout WPAT schools. Should information need to be accessed outside of the network, files must be saved in a specified OneDrive folder. This folder is only available for individuals that have been granted access to it and can be accessed via the internet anywhere. Files must not be downloaded to any device that hasn't been issued by WPAT.

Staff must not use memory sticks for the transfer of sensitive information. In the instances where the use of OneDrive is not available, only encrypted devices such as Iron key's should be used.

On the occasion where sensitive or personal information must be shared with an outside organisation, staff must use Egress or a One Drive shared folder to share the information.

In the situation where paper records must be transferred to another organisation or individual, if face to face deliver is unfeasible, information must be marked as confidential and sent by recorded delivery. Every feasible attempt to ensure safe delivery must be made.

3.6 Secure disposal or re-use of equipment

Appropriate arrangements are made for the secure disposal of media containing sensitive information. Confidential paper documents must be securely disposed of by shredding. Storage devices containing sensitive information must be destroyed or securely overwritten (rather than using the standard delete function) prior to disposal. Equipment containing storage media (e.g. hard disks) must be checked to ensure that sensitive data and licensed software have been removed or overwritten prior to disposal or reuse.

3.7 Clear desk and screen policy

Where appropriate, paper and computer media containing personal information must be stored out of sight when not in use. Sensitive printed material must be cleared from printers immediately and filed or shredded. PC's and laptops must be locked when left unattended. Users must terminate active sessions and log off and power down when finished to ensure that security patches are installed when available.

4 Communications and operations management

4.1 Operating procedures

System changes are managed through a controlled process, with major changes identified and documented after assessing their potential impact. Details of the changes are then communicated to the appropriate individuals. Incident management procedures are in place to ensure a quick, orderly and effective response to security incidents.

4.2 Installation of software

Microsoft Windows and Office 365 is installed and maintained by EDAC. Where additional software is required, written authorisation must be sought from the Headteacher of the school ahead of installation. Confirmation of this installation must be shared with the Data Protection Officer ahead of installation. Only software that is required for the job WPAT have employed an individual for is permitted to be installed.

Where software will make use of personal information, a Data Protection Impact Assessment must be completed ahead of purchase. Intention to utilise a new piece of software must be flagged with the Data Protection Officer as soon as possible in order to perform the assessment.

Software audits will be conducted throughout the year to ensure that only appropriate and active software is in use. Use of unlicensed software is prohibited. Any software found without appropriate permissions will be subject to investigation and disciplinary processes may be invoked if appropriate.

4.3 Housekeeping and network management

Back-up copies of all information stored on the network are taken every day. Backups are kept for a period of 90 days to ensure protection against dormant malware.

4.4 Electronic mail

WPAT emails must only be used in the context of WPAT business. Emails must not be sent that will bring the organisation or any member of staff within the organisation into disrepute. All measures

must be taken to ensure professionalism when constructing emails. WPAT email addresses must not be used when purchasing goods for private use.

When sending email to multiple addresses, the BCC field must be used in the situation where emails should not be shared with other people.

When emailing outside of the WPAT network, staff must ensure that no personal information is included in the email or in any attachments.

All emails sent and received using a WPAT 365 account remain the property of WPAT and as such may be accessed, without prior permission, in the event of a legitimate business need. This access would only be granted through a written request for permission to the DPO.

4.5 School trips/ educational visits

In the situations where physical copies of pupil information must be taken off site, all documentation must be signed out before leaving the premises. On return, these documents must be accounted for and signed back in. They must be destroyed in accordance with the document retention schedule.

5 Access control

5.1 User registration

Formal procedures are in place to control the allocation of access rights to information systems and services. Users have authorisation from the system owner and the level of access is appropriate for the purpose. User access rights are regularly reviewed; access rights of leavers are removed immediately and redundant user IDs removed. Privileges associated with each system and user are identified, allocated on a need-to-use basis and kept to a minimum.

5.2 User password management

Users must keep passwords confidential and avoid sharing them, keeping a paper record or recording them in a way that makes them accessible to unauthorised persons. Passwords must be over 8 digits long and include at least 1 number or special characters. If it is suspected that a password has been compromised, the password must be changed.

5.3 Systems development and maintenance

Security issues are identified and considered at an early stage when procuring or developing new information systems. Input data is validated to ensure that it is correct and appropriate. Outputs and downloaded or uploaded data are checked for validity and integrity.

6 Auditing of the policy

Regular checks will be made on emails that are sent outside of the WPAT network. These checks will be performed each month randomly focusing on different email traffic each time. This monitoring is to ensure that the policy is being adhered to with regard to sending personal information via email. Any concerns will be flagged with the WPAT Data Protection Officer and may lead to further investigation, where necessary.

All emails sent from the WPAT network are subject to monitoring to ensure that content is of an appropriate nature. Any emails highlighted as part of this monitoring will be investigated by the WPAT Data Protection Officer.