Pickwick Academy Trust

Data Protection Policy

Policy Group:	**Admin & Data**
Policy Ref:	**ADD/03**
Responsible Reviewing Officer and Job Title:	**Emma Oldale, CFOO** **i-West, DPO**
Date Written:	**October 2025**
Date Approved by the Board:	**October 2025**
Date of Next Review:	**October 2027 or earlier if an update made by our DPO**

Contents

1. Introduction 3
2. Scope 3
3. Definitions 3
4. Roles and Responsibilities 5
5. Data Protection Officer (DPO) 7
6. Data Subject Rights 7
7. Data Protection Principles 9
8. Processing Personal Data 12
9. Third Parties with Access to Personal Data 14
10. Data Protection by Design and Default 15
11. Personal data breaches or near misses 16
12. Destruction of records 16
13. Training 16
14. Monitoring Arrangements 16
15. Complaints 17
16. Legislation and Guidance 17
17. Links with Other Policies 18

Appendix 1 – Examples of Special Category Data that we process 19

Appendix 2 – Subject Access Request Procedure (SAR) 20

1. Introduction

a. The Trustees and the Executive Team of Pickwick Academy Trust are committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).
b. Pickwick Academy Trust are registered as a data controller with the Information Commissioner.
c. The details of Pickwick Academy Trust's Data Protection Officer can be found in Section 5.
d. This policy is available on Pickwick Academy Trust's website and in hard copy.

2. Purpose and Scope

a. This policy applies to anyone who has access to and/or is a user of Pickwick Academy Trust ICT systems, both in and out of Pickwick Academy Trust, including staff, governors, pupils, volunteers, parents / carers, visitors, contractors, and other community users.
b. This policy is also intended to serve as the appropriate policy document for the processing of Special Category Data and Criminal Record Data (where applicable).
c. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3. Definitions

a. **Personal data** - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. Pickwick Academy Trust may process a wide range of personal data of staff (including governors and volunteers) pupils, their parents or guardians as part of its operation. A non-exhaustive list of examples of the types of personal data that we process may be found in our Privacy Notices.

This personal data may include (but is not limited to):

- Names and addresses (including email addresses)
- Bank details
- Academic data e.g. class lists, pupil progress records, reports, disciplinary actions, admissions and attendance records
- References
- Employment history
- Taxation and national insurance records
- Appraisal records

- Examination scripts and marks

b. **Special category personal data** – Formally known as ‘sensitive personal data’, special category data is information which is more sensitive and so needs more protection. Categories fora living individual are:

   - Racial or ethnic origin
   - Political opinions
   - Religious or philosophical beliefs
   - Trade union membership
   - Genetics
   - Biometrics (such as fingerprints, retina and iris patterns, voice biometrics), where used for identification purposes
   - Health – physical or mental
   - Sex life or sexual orientation

     Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as does our Privacy Notice which may be found on our website. Examples of the types of special category data we hold are found at Appendix 1.

c. **Data Processing** - Data Processing is an over-arching term that means “doing something” with personal data. This commonly includes:

   - Collecting or collating the data
   - Analysing the data
   - Sharing the data
   - Storing the data
   - Destroying the data

d. **Data Subject** - The identified or identifiable (living) individual about whom the personal data relates or identifies and whose personal data is therefore held or processed.

e. **Data Controller** - The Data Controller is occasionally the person or more commonly the organisation with overall responsibility for the processing of personal data that organisation undertakes. They will make all the decisions about what is captured, how it’s used and the purpose for it, as well as deciding what controls need to be in place.

f. **Data Processor** - is occasionally a person, but more commonly an organisation commissioned by a Data Controller to carry out their data processing on behalf of the Data Controller. These are usually software providers such as Microsoft, or contracted out services such as an insurance company. Essentially, a Data Processor is acting as an extension of the Data Controller, so must operate under the Data Controller’s instructions, and under the terms of a Data Processing Agreement (contract).

g. **Data Breach** - The most common type of data breach is the accidental or unlawful *loss, alteration, destruction, disclosure of or access to* personal data, for example sending an email to the wrong recipient, losing a file containing personal data, or

sharing passwords enabling someone else to access your account. However, you should consider any failing of one of the Data Protection Principles (Article 5 of GDPR) as a GDPR breach, this could include examples such as not having the necessary paperwork in place, not providing the data subject with clear privacy information, retaining personal data for longer than is necessary or processing personal data without an identified lawful basis (Article 6 of GDPR).

h. **Data Sharing** - means *giving* it to another Data Controller, for them to use for their own purposes. Once you have shared personal data, the recipient becomes the Data Controller for that information, and therefore makes the decisions over what they will do with it.

Note, we do NOT share data with our Data Processors, as these are processing it under your Data Controllership.

i. **Data Processing Agreement –** a legally binding contract between the Data Controller and its Data Processor. This contract defines exactly how the Data Controller expects the Data Processor to process its personal data, and follow standard contract clauses.

j. **Data Sharing Agreement** – a non-legally binding written agreement between Data Controllers where there is regular sharing of personal data. The Sharing Agreement should define who is involved in the agreement, what data is being shared, why the recipient needs the data, how this is lawful, the how the data will be shared.

4. Responsibilities and Accountabilities

a. The Trust Board has overall responsibility for ensuring that Pickwick Academy Trust complies with all relevant data protection obligations and is responsible for reviewing and approving this policy

b. The CEO is responsible for the broadcast of this policy across the trust and for its promulgation through the CFOO, Directors of Education and Executive Headteachers and central team Heads of Department.

c. The CFOO acts with the delegated authority of the Trust Board on a day to day basis as internal Data Protection Lead and will liaise with the DPO. In the CFOO's absence, in case of emergency, this role will be delegated to the CEO.

d. Headteachers are responsible for the policy's implementation in each of the Trust's schools.

e. The CFOO is responsible for the implementation of this policy within the trust Central Team .

f. All staff are responsible for:

- Familiarising themselves with and complying with this policy and acceptable use policies for staff. The learning culture within the organisation seeks the

avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;

- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Only using computers and other devices authorised by Pickwick Academy Trust for accessing and processing personal data ensuring that they are properly "logged-off" at the end of any session in which they are using personal data; **and locking devices when they are temporarily left unattended at any point (Windows Button + L is a handy shortcut);**
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite (unless in accordance with the guidelines in Section 7) or to personal devices.
- Deleting data in line with this policy, the Records Management Policy and the retention schedule;
- Informing Pickwick Academy Trust of any changes to their personal data, such as a change of address;
- Reporting to their Headteacher, or the CFOO for those in the Pickwick Central Team, or in their absence the DPO in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK and European Economic Area;
    - The discovery of a data breach or near miss (**immediate action is required**) – please refer to the Data Breach Policy and Section 11 of this policy;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to be required and potentially a data protection impact assessment, please see - *Sharing Personal Data* (See Section 9).

5. Data Protection Officer (DPO)

a. The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law,

providing support and developing related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance directly to the Board of Trustees and, where relevant, provide Pickwick Academy Trust with advice and recommendations on data protection issues.

b. Pickwick Academy Trust has appointed i-West as its DPO, and they can be contacted through:

Email: i-west@bathnes.gov.uk

Telephone: 01225 395959

One West
Bath and North East Somerset Council
Guildhall
High Street
Bath
BA1 5AW

Under usual circumstances the Head of Governance and Compliance will be the point of contact with the DPO, with any significant issues raised with the CFOO.

6. Data Subject Rights

In all aspects of its work, Pickwick Academy Trust will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of the Trust's work. Subject to exceptions, the rights of the data subject as defined in law are:

a) The Right to be informed.

Pickwick Academy Trust advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation, such as data capture and consent forms where appropriate.

b) The Right of access

An individual when making a subject access request (SAR) is entitled to the following;

i. Confirmation that their data is being processed;
ii. Access to their personal data;
iii. Other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

Pickwick Academy Trust must respond to such a request within one calendar month unless the request is complex, in which case it may be extended by a further 2 calendar months. Please refer to Appendix 2 for further details as to how to manage a subject access request.

c) The Right to rectification

Individuals have the right to ask us to rectify information that they think is inaccurate or incomplete. Pickwick Academy Trust has a duty to investigate any such claims and

rectify the information where appropriate within one calendar month, unless an extension of up to a further 2 calendar months can be justified.

d) The Right to erasure

Individuals have a right to request that their personal information is erased but this is not an absolute right. It applies in circumstances including where:

- The information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
- The information is no longer required by Pickwick Academy Trust;
- A legal obligation to erase the data applies;
- The data was collected from a child for an online service or
- The trust has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of the school to continue to process it.

Pickwick Academy Trust will consider such requests as soon as possible and within one month, unless it is necessary to extend that timeframe for a further two months on the basis of the complexity of the request or a number of requests have been received from the individual.

e) The Right to restrict processing

This is not an absolute right. An individual may ask the Trust to temporarily limit the use of their data (for example store it but not use it) when it is considering:

- A challenge made to the accuracy of their data, or
- An objection to the use of their data.

In addition, Pickwick Academy Trust may be asked to limit the use of data rather than delete it:

- If the individual does not want Pickwick Academy Trust to delete the data but does not wish it to continue to use it;
- In the event that the data was processed without a lawful basis;
- To create, exercise or defend legal claims.

f) The Right to data portability

An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. Pickwick Academy Trust only has to provide the information where it is electronically feasible.

g) The Right to object

Individuals have a right to object in relation to the processing of data in respect of:

- a task carried out in the public interest except where personal data is processed for historical research purposes or statistical purposes
- a task carried out for the exercise of official authority
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or
- direct marketing.

Only the right to object to direct marketing is absolute, other objections will be assessed in accordance with data protection principles. Pickwick Academy Trust will advise of any decision to refuse such a request within one month, together with reasons and details of how to complain and seek redress.

h) Right to complain

Individuals have the right to complain about the way in which an organisation processes their personal data. This is the first stage, before the Information Commissioner will consider a personal data complaint. We have provided a webform for individuals to make a complaint, which can be found Here

i) Rights related to automated decision making

This does not apply as Pickwick Academy Trust does not employ automated decision-making processes.

7. Data Protection Principles

a. Data Protection Legislation is based on 7 key data protection principles that Pickwick Academy Trust complies with.

b. The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – Pickwick Academy Trust will explain to individuals why it needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). Pickwick Academy Trust reviews its documentation and the basis for processing data on a regular basis.

- **Collected for specified, explicit and legitimate purposes** – Pickwick Academy Trust explains these reasons to the individuals concerned when it first collects their data. If Pickwick Academy Trust wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information. Pickwick Academy Trust will document the basis for processing.

- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed** – Pickwick Academy Trust must only process the minimum amount of personal data that is necessary in order to undertake its work.

- **Accurate and, where necessary, kept up to date** – Pickwick Academy Trust will check the details of those on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.

- **Kept for no longer than is necessary for the purposes for which it is processed** – We review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed). When Pickwick Academy Trust no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the retention schedule. We only keep personal data, including special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;

    - We have a records management policy which governs how long all data including special category data shall be retained for. This policy is complied with and reviewed regularly;
    - Once the data is no longer needed, we delete it, securely destroy it in line with our records management policy, or render it permanently anonymous.

- **Processed in a way that ensures it is appropriately secure** – Pickwick Academy Trust implements appropriate technical measures to ensure the security of data and systems for staff and all users. Please refer to the Information Security Policy, and how data is securely transferred in and out of Pickwick Academy Trust's system.

    - We adopt a risk- based approach to taking data offsite. Unless absolutely necessary, hard copies of special category personal data will not be removed from our premises.
    - Any decision to remove the information must be based on the business need of the organisation or in the best interests of the individual, rather than for the convenience of the individual member of staff. It is always preferable for any special category personal data to be accessed via an appropriately encrypted means rather than via hard copy, when off-site.

- If there is no reasonable alternative to removing hard copies from the the schools within Pickwick Academy Trust, the following procedure will apply:

    i. A record of what information has been removed will be logged on site with the office so that there is a record of what has been removed – for example health data in trip packs;
    ii. Information will be transported and stored securely at all times, the method of which will depend on the level of sensitivity and category of data;
    iii. Wherever possible, information that is removed from site will be pseudonymised by using a "key" held by the office on site, such as initials or a colour coded key identification system and the trust/ school logo removed;
    iv. We adopt a risk- based approach, for example hard copy personal data with lower sensitivity (e.g. exercise books) may be taken off site, but if left in a vehicle must be locked in the boot, never left in a visible place, only for the shortest period of time and never overnight. Special Category Data (e.g. SEND, Safeguarding, Health data) must be kept on the staff member's person at all times.
    v. Special category data must be returned to the school or Trust's premises at the end of the working day, if not on a residential school trip. If this is not practicable, and a staff member needs to retain the information in their personal possession, this must be discussed in advance with a member of the trust Executive Team or school Senior Leadership Team (SLT) including what measures will be taken to safeguard the information, given the risks that are beyond a staff member's control in so doing and the potential consequences ensuing. The relevant member of the SLT must record their decision.
    vi. Data will be tidied away when not in use (e.g. when staff undertake marking at home, it must be out of sight of family members, not left out and tidied away afterwards).
    vii. Only those who have need to access the data concerned will be granted permission and access to it.
    viii. Our acceptable use policies describe the requirements around bring your own device, remote working and password protection.

- **Accountability –** Pickwick Academy Trust complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy including completing Data Protection Impact Assessments (DPIAs) where necessary; integrating data protection into internal documents including this policy, any related policies and Privacy

Notices; regularly training members of staff on all relevant data protection law, including this and any related policies; reviewing and auditing privacy measures and compliance; maintaining and reviewing records of its processing activities for all personal data that it holds; reviewing and ensuring familiarity of policies related to the handling of data; reviewing reasons for data breaches; and ensuring stakeholders manage risks and compliance using the trust Risk Register.

8. Processing Personal Data

a. In order to ensure that Pickwick Academy Trust's processing of personal data is lawful; it will always identify one of the following six grounds for processing **before** starting the processing:

- The data needs to be processed so that Pickwick Academy Trust can fulfil a **contract** with the individual, or the individual has asked Pickwick Academy Trust to take specific steps before entering into a contract;
- The data needs to be processed so that Pickwick Academy Trust 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 Pickwick Academy Trust, 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 Pickwick Academy Trust or a third party where necessary, balancing the rights of the individual, (unless the processing is necessary for a 'recognised' legitimate interest). However, where Pickwick Academy Trust can use the public task basis for processing, it will do so rather than rely on legitimate interests as a basis for processing.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent. In the case of **special categories of personal data**, this must be **explicit consent.** Pickwick Academy Trust will seek consent to process data from the pupil or parent/carer depending on their age and capacity to understand what is being asked for.

8.1 Processing Special Categories of Personal Data

In addition to the legal basis to process personal data, special categories of personal data also require an additional condition for processing under Article 9 of the GDPR. The grounds that we may rely on include:

a) The individual has given **explicit consent** to the processing of those special categories of personal data for one or more specified purposes;

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment, health and social security and social protection law and research**; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018.

c) Processing is necessary to protect the **vital interests** of the individual or of another natural person where the individual is physically or legally incapable of giving consent;

d) Processing relates to personal data which are manifestly **made public** by the individual;

e) Processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;

f) Processing is necessary for reasons of **substantial public interest** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision-making process.
These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

- Statutory and government purposes
- Safeguarding of children or individuals at risk
- Legal claims
- Equality of opportunity or treatment
- Counselling
- Occupational pensions

g) Processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in section 8;

h) Processing is necessary for reasons of **public interest in the area of public health;**

i) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the Data Protection Officer where appropriate.

We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest.

8.2 Legal basis for processing criminal offence data

a. Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

We do not maintain a register of criminal convictions.

b. When processing this type of data, we are most likely to rely on one of the following bases:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection;
- The processing is necessary for the purposes of protecting the physical, mental or emotional well-being of an individual;
- The processing is necessary for statutory purposes; or
- Consent – where freely given. Pickwick Academy Trust acknowledges because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid and will only rely on this where no other ground applies.

9. Third Parties with Access to Personal Data

a. Please refer to the Trust's Privacy Notice(s) for details of who, aside from the school/Trust, has access to the personal data processed.

9.1 Data Sharing

Pickwick Academy Trust will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:

- Pickwick Academy Trust will share data if there is an issue with a pupil, individual or, parent/carer that puts the safety of staff or others at risk;
- Pickwick Academy Trust will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where child protection and safeguarding concerns apply, it will apply the "Seven golden rules of information sharing." In limited circumstances, data may be shared with external agencies without the knowledge or consent of the parent or pupil in line with the DPA 2018, which includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent;

Pickwick Academy Trust may also disclose personal data to law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:

- For the prevention or detection of crime and/or fraud;
- For the apprehension or prosecution of offenders;
- For the assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- For research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided or it is otherwise fair and lawful to do so.

Pickwick Academy Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects pupils/ or staff.

9.2 Third-Party Processors

Pickwick Academy Trust's suppliers and contractors including its Data Protection Officer and IT provider may need data to provide services. When third parties are processing personal data on behalf of Pickwick Academy Trust, we will:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law;
- Establish a data processing contract 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 it shares;
- Only provide access to data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with Pickwick Academy Trust.

10. Data Protection by Design and Default

a. Pickwick Academy Trust has a legal obligation to integrate appropriate technical and organisational measures into all of its processing activities, and to consider this aspect before embarking on any new type of processing activity.

b. It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity i-west must be consulted and an initial screening be conducted assessing risk.

c. Please refer to the Information Security Policy for further detail as to how Pickwick Academy Trust implements this principle in practice.

11. Personal data breaches or near misses

a. A personal data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service."* It may be deliberate or accidental.

b. Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the staff member must inform the Headteacher, CFOO and DPO **immediately** in order that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

c. Further details on security incidents and data breaches can be found in the trust Data Breach Policy.

12. Destruction of records

a. Pickwick Academy Trust adheres to its Records Management Policy and will permanently securely destroy both paper and electronic records securely in accordance with these timeframes.

b. Pickwick Academy Trust will ensure that any third party who is employed to perform this function has the necessary accreditations and safeguards.

c. Where Pickwick Academy Trust deletes electronic records and its intention is to put them beyond use, even though it may be technically possible to retrieve them, it will follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

13. Training

a. To meet its obligations under Data Protection legislation, Pickwick Academy Trust will ensure that all staff, volunteers, Trustee's, and Governors receive an appropriate level of data protection training as part of their induction. Those who have a need for additional training will be provided with it, for example relating to use of systems or as appropriate, at least every two years.

b. Data protection also forms part of continuing professional development, and updates will be provided where changes to legislation, guidance or Pickwick Academy Trust's processes make it necessary. This may include lessons learned from data breaches and near misses and preventative measures to

avoid them, alongside other best practice advised, for example adding a one or two minute delay to emails.

14. Monitoring Arrangements

a. Whilst the DPO is responsible for advising on the implementation of this policy and monitoring Pickwick Academy Trust's overall compliance with data protection law, Pickwick Academy Trust is responsible for the day to day implementation of the policy and for making the data protection officer aware of relevant issues which may affect the trust's ability to comply with this policy and the legislation.

b. This policy will be reviewed annually, unless an incident or change to regulations or to the DPO dictates a sooner review.

15. Complaints

a. Pickwick Academy Trust is always seeking to implement best practice and strives for the highest standards. The Trust operates an "open door" policy to discuss any concerns about the implementation of this policy or related issues. Pickwick Academy Trust's complaints policy may be found on its website.

c. Individuals have the right to make a complaint to use about the way in which we process personal data. There is also a right to make a complaint to the Information Commissioner, but complaints should be raised with us first by contacting governance@pickwickacademytrust.co.uk

d. We will acknowledge your complaint within 30 days and respond without undue delay.

We have provided a webform for individuals to make a complaint, which can be found Here

Please complete the form and return via email to governance@pickwickacademytrust.co.uk

The ICO is contactable at:

Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.

Telephone: 0303 123 1113

16. Legislation and Guidance

This policy takes into account the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office
  Information Sharing – Advice for Practitioners – DfE July 2018

17. Links with Other Policies

This Data Protection Policy is linked to the following:

- Information Security Policy
- Records Management Policy
- Data Breach Policy
- Privacy Notices
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Consent / Permissions Forms
- Admissions Form

Appendix 1 – Examples of Special Category Data that we process

Examples of where we may process special category data include in

- Pupil health data and information concerning their racial / ethnic origin in admissions records and in pupil records / trip packs
- Special Educational Needs information
- School census information
- Attendance records
- Information contained within child protection and safeguarding records
- Staff application forms
- HR files including and disciplinary and capability proceedings which may include DBS, and right to work checks, health, and equal opportunities data (disability, race, ethnicity, sexual orientation).
- Employee Health Data and information concerning their racial/ ethnic origin
- Accident reporting documentation

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as does our Privacy Notice which may be found on our website.

Appendix 2 – Subject Access Request Procedure (SAR)

Staff at Pickwick Academy Trust shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) following advice and guidance provided by its Data Protection Officer (i-west).

1. Ascertain whether the requester has a right to access the information and capacity.
2. Obtain (reasonable and proportionate) proof of identity
3. Engage with the requester if the request is too broad or needs clarifying (once steps two and three have been completed, the 'clock' can start.
4. Make a judgement on whether the request is complex and therefore can be extended by an additional 2 months
5. Acknowledge the requester providing them with
    a. the response time – 1 month (as standard), an additional 2 months if complex; and
    b. details of any costs – Free for standard requests, or you can charge, or refuse to process if the request is manifestly unfounded or excessive, or further copies of the same information are required, the fee must be in line with the administrative cost
6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held
7. Collect the data (the organisation may use its IT support to pull together data sources such as emails and databases–
8. If (6) identifies third parties who process it, then engage with them to release the data to Pickwick Academy Trust.
9. Review the identified data for exemptions and redactions in line with the ICO's Guide to the Right of Access and in consultation with the Pickwick Academy Trust's Data Protection Officer (One West),
10. Create the final bundle and check to ensure all redactions have been applied
11. Submit the final bundle to the requester in a secure manner and in the format they have requested.