Data Protection Policy (incorporating special categories)

If you require help with the interpretation of this policy, please email the Data Protection Officer at

DPO@st-margarets.torbay.sch.uk

Reviewed Annually – Latest Review Autumn Term 2026

Contents

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

Appendix 1 – Examples of Special Category Data that we process 15

Appendix 2 – Subject Access Request Procedure (SAR) 16

1. Aims

The Trustees and Senior Leadership Team (SLT) of St Margaret's Academy are committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws. This includes the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018 (DPA 2018)**, and the **Data (Use and Access) Act 2025 (DUAA)**

The Academy are registered as a data controller with the Information Commissioner.

The details of the Academy's Data Protection Officer can be found at paragraph 5.

2. Scope

This policy applies to all personal data, regardless of format (paper or electronic). It applies to anyone who has access to or uses Academy ICT systems, both on and off-site, including staff, trustees, pupils, volunteers, parents/carers, visitors, contractors, and community users.

3. Distribution

This policy is available on the Academy's website and can be printed on request.

4. Definitions

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. The Academy may process a wide range of personal data of staff (including trustees and volunteers) pupils, their parents or guardians as part of its operation.

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 / pupil progress records, reports, disciplinary actions, admissions and attendance records
- References
- Employment history
- Taxation and national insurance records
- Appraisal records
- Examination scripts and marks

Special category personal data

Highly sensitive personal data requiring enhanced protections under UK law. This includes racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometrics (where used for identification), health data, and data concerning an individual's 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 may be found at appendix 1.

Processing - Any operation performed on personal data, whether manual or automated, such as collection, recording, structuring, storage, alteration, retrieval, use, disclosure, or destruction.

Data subject - The identified or identifiable (living) 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.

5. Roles and Responsibilities

Board of Trustees - Holds ultimate accountability for ensuring the Academy complies with all UK data protection legislation.

Headteacher - The Headteacher acts with the delegated authority of the Board of Trustees on a day to day basis and will liaise with the DPO. In the Headteacher's absence, in case of emergency, this role will be delegated to Deputy Headteacher.

All staff - 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 the Academy 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;
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite (unless in accordance with the guidelines at paragraph 8 or to personal devices other than in accordance with the Academy’s Personal devices user agreement – pupils and staff
- Deleting data in line with this policy and the retention schedule;
- Informing the Academy of any changes to their personal data, such as a change of address;
- Reporting to the Headteacher, 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 page 9 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* (paragraph 9).

6. Data Protection Officer (DPO)

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 the Academy with advice and recommendations on data protection issues.

The Academy has appointed i-West as its DPO, and they can be contacted by email at:

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 internal data protection lead, Headteacher or a member of SLT will be the point of contact with the DPO.

7. Subject Access Requests and Other Rights of Individuals

The Academy safeguards individual rights under the UK GDPR, DPA 2018, and DUAA.

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

a) The Right to be informed.

The Academy 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.

The Academy 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. The Academy 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 the Academy;
- A legal obligation to erase the data applies;
- The data was collected from a child for an online service or
- The Academy 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 Academy to continue to process it.

The Academy 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 Academy 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, the Academy may be asked to limit the use of data rather than delete it:

- If the individual does not want the Academy to delete the data but does not wish to it 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. The Academy 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 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. The Academy 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) The Right to Complain

Individuals have the right to raise a complaint about the handling of their personal data directly with the Academy and may also lodge a complaint with the Information Commissioner.

i) The Right Relating to Automated Decision-Making

Individuals have rights in relation to solely automated decision-making and profiling where such processing produces legal or similarly significant effects. Any use of Artificial intelligence tools will be assessed to ensure compliance with data protection legislation and the rights of individuals.

8. Data Protection Principles

The GDPR is based on 7 key data protection principles that the Academy complies with.

The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – the Academy will explain to individuals why the Academy 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). The Academy reviews its documentation and the basis for processing data on a regular basis

- **Collected for specified, explicit and legitimate purposes** – the Academy explains these reasons to the individuals concerned when it first collects their data. If the Academy 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/ The Academy will document the basis for processing.

- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed -** the Academy 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** – the Academy 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 the Academy 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, include 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 retention and disposal 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 retention and disposal policy, or render it permanently anonymous.

- **Processed in a way that ensures it is appropriately secure** – the Academy implements appropriate technical measures to ensure the security of data and systems for staff and all users.

- **Accountability –** The Academy 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 the Academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data and CCTV. However, the Academy will liaise with the DPO who will advise on this process. Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually;
  - 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; the Academy also maintains a record of attendance;
  - Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and Academy policies;
  - Maintaining records of its processing activities for all personal data that it holds;

9. Lawful Bases for Processing Personal Data

In order to ensure that the Academy'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 the Academy can fulfil a **contract** with the individual, or the individual has asked the Academy to take specific steps before entering into a contract;
- The data needs to be processed so that the Academy 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 Academy, as a public authority, can **perform a task in the public interest, and carry out its official functions**;
- Processing may be carried out where it is necessary for the **legitimate interests** of the Academy or a third party, unless overridden by the rights and freedoms of the individual, or where processing is necessary for a recognised legitimate interest under applicable legislation.
- However, where the Academy can use the public task basis for processing, it will do so rather than rely on legitimate interests as the 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.** The Academy will seek consent to process data from the pupil / pupil or parent depending on their age and capacity to understand what is being asked for.

For **Special Category Data**, an additional condition under Article 9 of the UK GDPR must be met, such as explicit consent, employment/social protection law, or substantial public interest (e.g., child safeguarding under Schedule 1 of the DPA 2018)

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.

Health or social care purposes includes the following purposes:

i. Preventative or occupational medicine
ii. The assessment of the working capacity of the employee

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 paragraph 3
;

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 as follows:

Legal basis for processing criminal offence data

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

We do not maintain a register of criminal convictions.

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; or
- Consent – where freely given. The Academy 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.

10. Sharing Personal Data

Please refer to the Academy's Privacy Notices.

- We 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:

- We will share data if there is an issue with a pupil or third party, for example, parent/carer that puts the safety of staff or others at risk;
- We 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" which provide that in limited circumstances data may be shared with external agencies without the knowledge or consent of the parent or pupil;
- The Academy's suppliers and contractors including its data protection officer may need data to provide services. When sharing data, the Academy will:
  - Only appoint suppliers or contractors which 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 where there is regular sharing;
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Academy.

- The Academy may also share personal data with 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.

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

11. Data Protection by Design and Default

The Academy 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.

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.

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

12. Personal data breaches or near misses

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.

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the staff member must inform the Headteacher 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.

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

13. Destruction of records

We apply our retention policy and will permanently destroy both paper and electronic records securely in accordance with these timeframes.

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

If we delete electronic records and our intention is to put them beyond use, even though it may be technically possible to retrieve them, we 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.

14. Training

To meet our obligations under Data Protection legislation, we will ensure that all staff, volunteers, and Trustees 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.

Data protection also forms part of continuing professional development, and updates will be provided where changes to legislation, guidance or the Academy's processes make it necessary.

15. Monitoring Arrangements

Whilst the DPO is responsible for advising on the implementation of this policy and monitoring the Academy's overall compliance with data protection law, the Academy 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 Academy's ability to comply with this policy and the legislation.

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

16. Complaints

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

Data Protection complaints will be acknowledged and investigated without undue delay. Although you have a right to make a complaint to the Information Commissioner's Office (ICO), Individuals will be encouraged to raise concerns with the Academy in the first instance before escalating matters to the Information Commissioner.

The ICO is contactable at:

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

Telephone: 0303 123 1113.

17. Legislation and Guidance

This policy takes into account the following legislation and statutory guidance:

- The **UK General Data Protection Regulation (UK GDPR)**
- The **Data Protection Act 2018 (DPA 2018)**
- The **Data (Use and Access) Act 2025 (DUAA)**
- The **Protection of Freedoms Act 2012** (governing biometric data in Academys)
- Regulatory guidance published by the **Information Commission**
- **Protection of Biometric Information of Children in Academys and Colleges** (DfE guidance)
- **Information Sharing: Advice for Practitioners Providing Safeguarding Services** (DfE guidance)

18. Links with Other Policies

This Data Protection Policy is linked to the following:

- Information Security Policy
- Retention & Disposal Policy
- Personal Devices User Agreement
- Data Breach Policy
- Privacy Notices
- Safeguarding Policy
- Acceptable Usage Policies
- E-Safety/Online Safety Policy
- Consent / Permissions Form
- Admissions Form
- Data Protection Policy for Sign In App

Appendix 1 – Examples of Special Category Data that we process

- Pupil health data and information concerning their racial / ethnic origin in admissions records and in pupil records / trip packs
- Academy 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).
- 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)

The Academy shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer (i-west), using the Academy SAR Guidance provided to the Academy.

1. Ascertain whether the requester has a right to access the information and capacity.https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/?search=hold

2. Obtain proof of identity (once this step has been completed the clock can start)

3. Engage with the requester if the request is too broad or needs clarifying

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 is 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 – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)

8. If (6) identifies third parties who process it, then engage with them to release the data to the Academy.

9. Review the identified data for exemptions and redactions in line with the and in consultation with the organisation's Data Protection Officer (i-west), and their Academy SAR Guidance.

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.