Mae'r ddogfen hon hefyd ar gael yn Gymraeg

This document is also available in Welsh

DATA PROTECTION POLICY

Author	Director of Policy, Assurance and Compliance
Version	1.1
Status	Final
Date Approved	26.06.25
Approved by	Audit and Risk Committee
Effective Date	26.06.25
Date of Next Review	26.06.27
Responsibility for Review	Director of Policy, Assurance and Compliance
Equality and Welsh Language Impact Assessment	Y
Health and wellbeing implications considered	Y

Version	Date	Description	Amended/Reviewed by
1.0	15.04.25	Review of Data Protection Policy with policy updates.	Director of Policy, Assurance and Compliance
1.1	26.06.25	Audit and Risk Committee approved the policy to making it the final version.	Director of Policy, Assurance and Compliance

Table of Contents

1. Scope and Purpose

1.1: **Purpose**

The purpose of this Data Protection Policy is to establish the commitments of St David's Catholic College in relation to the protection of personal data. It exists to ensure that the college meets its legal, regulatory and ethical obligations when processing personal data and to support the development of a data protection culture that values privacy, accountability and transparency.

This policy provides the overarching framework for how the college will:

- Uphold the data protection principles set out in the UK General Data Protection Regulation (UK GDPR), ensuring that personal data is processed lawfully, fairly, transparently and is collected for specified purposes; limited to what is necessary; is accurate and kept up to date; is retained only for as long as necessary and is handled securely.
- Respect and enable the rights of data subjects including their right to access, rectification, erasure, restriction, objection, data portability and to be informed about how their personal data is used.
- Ensure the college understands its information assets and processing activities through the maintenance of an *IAR and ROPA Register* with clear roles and responsibilities for data handling across departments.
- Ensure effective use of Data Protection Impact Assessments (DPIAs).
- Embed data protection considerations in all areas of activity developing an approach that demonstrates a data protection by design culture.

This policy is a key part of the college's overall governance of information and forms the basis for more detailed technical and procedural guidance in relation to data protection.

1.2: **Scope**

This policy applies to all processing of personal data carried out by or on behalf of St David's Catholic College, regardless of format (digital or paper), system (local or cloud-based) or location (on-site or remote). It applies to both automated and manual processing of data.

This policy applies to:

- All members of staff
- Senior Leadership and governors
- Agency and temporary staff
- Data Processors

This policy applies to all personal data processed in the college including, but not limited to:

- Student records
- Staff Records
- Alumni Records
- CCTV and access control
- Communications
- Any processing involving special category data or criminal convictions data

1.3: **Links with related policies and procedures**

This policy aligns with and support a range of college policies and procedures to ensure a unified approach to data and records management. It should be read in conjunction with:

- Data Protection – IAR and ROPA Procedures
- Data Protection – Subject Access Request Procedures
- Data Protection – Subject Right Request Procedures
- Privacy Notices
- Data Breach Policy and Procedure
- Records Management Policy and Procedure
- IT Policy – Internal Systems
- Safeguarding Policy
- Equality and Diversity Policy
- Capabilities Policy
- Disciplinary Policy

1.4: **Relevant legislation and regulatory frameworks**

This policy is designed to comply with key legislation, regulatory frameworks and government and industry guidance including:

- UK General Data Protection Regulations (UK GDPR)
- Data Protection Act 2018
- ICO Guidance and Codes of Practice

2. Definitions

2.1: **Personal Data**: Any information relating to an identified or identifiable natural living person (the data subject).
2.2: **Special Category Data**: A sub-category of personal data that includes more sensitive information such as race, health, religious beliefs or sexual orientation which requires additional safeguards.
2.3: **Data Subject**: The individual to whom the personal data relates.
2.4: **Processing**: Any operation or set of operations performed on personal data including collection, storage, use, sharing and deletion.
2.5: **Data Controller**: The individual or organisation that determines the purposes and means of processing personal data.
2.6: **IAR (Information Asset Register) and ROPA (Record of Processing Activities)**: A record that documents the types of personal data held by the college and the purposes for processing including the lawful basis.

3. Policy Statement

3.1: Key Principles

The college approach to data protection is based on the seven Data Protection Principles as set out under UK GDPR:

- **Lawfulness, Fairness and Transparency:** The college will ensure it has a valid legal basis for collecting and using personal data, act fairly and inform individuals about the processing activities.
- **Purpose Limitation:** St David's Catholic College will ensure that personal data is collected for a specific, explicit purposes and not reuse the data in incompatible ways.
- **Data Minimisation:** Only personal data that is adequate, relevant and necessary shall be collected and processed.
- **Accuracy:** The college will strive to ensure that personal data is accurate and up to date and take reasonable steps to correct or erase data if it is incorrect or misleading.
- **Storage Limitations:** Personal data shall only be kept as long as necessary for the lawful basis on which it was collected.
- **Integrity and Confidentiality:** St David's College will strive to ensure that personal data is protected from unauthorised access, loss or disclosure.
- **Accountability:** the college will commit to take responsibility for the personal data collected and processed and ensure there are appropriate policies and procedures in place to record and demonstrate compliance.

3.2: Key Commitments

St David's Catholic College commits to:

3.2(i) Ensuring lawful, fair and transparent processing

- Only process personal data where a lawful basis applies.
- Creating, publishing and reviewing Privacy Notices for applicants, students and staff to ensure they understand what personal data is collected, the purpose for processing and the lawful basis on which the data is processed.
- Reviewing information collected and processing activities to ensure that Privacy Notices are accurate and up-to-date (see *Data Protection Procedures – IAR and ROPA*)

3.2(ii) Purpose Limitation

- Identifying and documenting the processing activities and their purposes by creating, maintaining and reviewing an IAR and ROPA Register (see *Data Protection Procedures – IAR and ROPA*).
- Regular reviews of the personal data collected and processing activities to prevent function creep (see *Data Protection Procedures – IAR and ROPA*).

3.2(iii) Data Minimisation

- Only collect personal data that is necessary for the purposes stated within the Privacy Notices and *IAR and ROPA Register*.
- Ensure that Data Protection Impact Assessments (DPIA) are completed for new procedures or systems to challenge any unnecessary processing of personal data during the design of those procedures or systems (see *Policy and Procedures Creation Process*).
- Complete annual reviews of the *IAR and ROPA Register* to ensure only necessary and relevant personal data is collected and, where sensitive data, a DPIA has been completed to challenge the processing activity (see *Data Protection Procedures – IAR and ROPA*).

3.2 (iv) Accuracy

- Provide mechanisms for individuals to correct inaccuracies in personal data.

3.2(v) Storage Limitations

- Create, maintain and regularly review the *Records Retention Schedule* as set out in the *Records Management Policy* and *Procedures.*
- Ensure responsible and secure record disposal in line with the *Record Retention Schedule* as documented in the *Records Disposal Register*. The college will investigate, document, report and take action where there is an accidental deletion of a record as set out in *Records Management Policy* and *Procedures* and, where it includes personal data, comply with *Personal Data Breach Policies and Procedures*.
- Track and monitor the implementation of the *Record Retention Schedule* to ensure compliance by carrying out regular audits as set out in the *Records Management Policy* and *Procedures*.

3.2(vi) Integrity and Confidentiality

- Monitor and report data breaches as set out in the *Personal Data Breach Policy* and *Procedures* and in line with UK GDPR and ICO guidance.
- Record, track, mitigate and implement actions to stop recurrence where a data breach takes place ensuring appropriate reporting to SLT and relevant Committees as set out in *Personal Data Breach Policy* and *Procedures* and the *Personal Data Breach Register.*
- Ensure the processing of special category and sensitive data is identified (through the *IAR and ROPA Register)*, security relating to the processing of that data is regularly reviewed including the completion of DPIA as required.

3.2(vii) Accountability

- Require mandatory annual staff compliance training related to GDPR.
- Ensure recording of all data protection events and report to senior leadership and relevant Committees.
- Conduct internal audits and governance reviews to ensure compliance with the relevant policies and procedures.

3.3: Commitment to the Rights of Data Subjects

St David's Catholic College is committed to supporting data subjects access their rights as set out under UK GDPR and the Data Protection Act 2018.

These rights include:

- Right to be Informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability
- Right to Object

The college is committed to receive requests in relation to these rights in a range of different formats, to document the request and the response to the request as well as report to senior leadership and relevant Committees.

To support data subjects in accessing these rights they will be promoted within Privacy Notices with a reporting process for ease of access.

In addition, please see *Data Protection Procedures – Rights of Data Subjects, Data Protection Procedures – Subject Access Requests* and *Records Management Policy* and *Procedures*.

3.4: Misuse of Data

Any member of staff, student of other stakeholder who considers that the policy has not been followed in respect of personal data about themselves should raise this with the data protection team by emailing DataProtection@stdavidscollege.ac.uk who will investigate and respond. It is also possible to raise a concern with the Information Commissioner's Office (ICO - Information Commissioner's Office)

4. Responsibilities

Data protection is a shared responsibility. While day-today operational responsibilities may be delegated, overall accountability lies with the college as the data controller. The following roles support this accountability structure:

4.1: **Governors**

- Provide strategic oversight and ensure that data proception forms part of the college's risk and compliance agenda.
- Support a culture of accountability and ensure appropriate resourcing for compliance.
- Receive regular reports on data protection risks, incidents and compliance monitoring.

4.2: **Senior Leadership Team (SLT)**

- Ensure data protection principles are embedded across strategic planning and operational leadership.
- Oversee compliance with data protection policies and procedures within their areas of responsibility.

4.3: **Director of Policy, Assurance and Compliance (also the DPO)**

- Advice the college and monitor compliance with data protection legislation.
- Serve as the primary point of contact for the Information Commissioner's Office (ICO) and data subjects.
- Lead the development, implementation and review of data protection policies, training and DPIAs and audit processes.
- Provide independent advice to SLT and Governors and raise concerns directly where required.

4.4: **Head of IT**

- Ensure technical and organisational security measures are in place to protect personal data.
- Lead the implementation of secure infrastructure and access controls.
- Collaborate with the Director of Policy, Assurance and Compliance in relation to new systems and technologies.
- Support incident response and recovery in the event of data breaches.

4.5: **Deans, Directors, Departmental Managers and Learning Area Leads**

- Ensure compliance with data protection policies with their areas.
- Maintain up-to-date IAR and ROPA records.
- Oversee the completion of DPIAs for new projects or systems in their area.
- Promote awareness and training for staff and ensure appropriate handling and secure storage and disposal of personal data.

4.6: **All Staff**

- Understand and comply with the college's data protection policies and procedures.
- Complete mandatory GDPR training and follow best practices for handling personal data.
- Report data protection concerns promptly to the Director of Policy, Assurance and Compliance.
- Process personal data only for the authorised purposes and in accordance with the principle of data minimisation and storage limitation.

5. Equality and Welsh Impact Assessment Statement

An Equality and Welsh Language Impact Assessment has been completed and it has been determined that there is an overall positive impact on these areas. In relation to equality the policy is applied universally, therefore, there are no barriers for individuals in protected groups accessing their rights under data protection. In addition, the rights-based approach and transparency created in relation to data processing supports the elimination of discrimination and advances equality of opportunity e.g. the ability to access and correct data can help to prevent discrimination. The policy and Privacy Notices will be available in Welsh and, as per the Welsh Language Policy, bilingual communication will be available as required.

6. Communication and Storage

6.1: This policy will be published to staff on the 'Every' platform.

6.2: This policy will be published to students, parents, guardians and other stakeholders on the college website.

6.3: This policy will be available in Welsh.