SIDMOUTH COLLEGE

Data Protection Policy

Policy adopted by the Full Governing Board: 1st July 2020

believe • inspire • succeed

Policy version: **1.2 July 2020**

Policy review date: **July 2022**

If you require help with the interpretation of this policy, please email the Data Protection Officer at dpo@sidmouthcollege.devon.sch.uk

Contents

1 Introduction and purpose

1.1 This policy sets out Sidmouth College's commitment to handling personal data in line with the EU General Data Protection Regulation 2016 and the UK Data Protection Act 2018 (collectively referred to as the data protection legislation).

1.2 The College is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO) under registration number Z7451862. Details about this registration can be found at www.ico.org.uk

1.3 The purpose of this policy is to explain how the College handles personal data under the data protection legislation, and to inform employees and other individuals who process personal data on the College's behalf, of the College's expectations in this regard.

2 Scope

2.1 This policy applies to the processing of personal data held by the College. This includes personal data held about students, parents/carers, employees, temporary staff, governors, visitors and any other identifiable data subjects.

2.2 This policy should be read alongside the Data and Information Security Policy, Online Safety Policy, Staff and Visitor Acceptable Use Policy and the Student Acceptable use Policy.

3 Definitions

3.1 There are several terms used in the data protection legislation and in this policy, which must be understood by those who process personal data held by the College. These are:

- Personal data
- Special categories of personal data
- Processing
- Data subject
- Data controller
- Data processor

3.2 These terms are explained in Appendix 1.

4 Roles and responsibilities

4.1 Governing Body

4.1.1 The governing body has overall responsibility for ensuring the College implements this policy and continues to demonstrate compliance with the data protection legislation.

4.1.2 This policy shall be reviewed by the governing body on an annual basis.

4.2 Principal

4.2.1 The Principal has day-to-day responsibility for ensuring this policy is adopted and adhered to by employees and other individuals processing personal data on the College's behalf.

4.3 Data Protection Officer

4.3.1 The Data Protection Officer (DPO) is responsible for carrying out the tasks set out in Article 39 of the General Data Protection Regulation (the GDPR). In summary, the DPO is responsible for:

- informing and advising the College of their obligations under the data protection legislation
- monitoring compliance with data protection policies
- raising awareness and delivering training to employees
- carrying out audits on the College's processing activities
- providing advice regarding Data Protection Impact Assessments and monitoring performance
- co-operating with the Information Commissioner's Office
- acting as the contact point for data subjects exercising their rights

4.3.2 The DPO shall report directly to the governing body and Senior Leadership Team and shall provide regular updates on the College's progress and compliance with the data protection legislation.

4.3.3 The College's DPO is an external consultant who performs the role under a service contract. The DPO is Amber Badley, who can be contacted through the College at dpo@sidmouthcollege.devon.sch.uk or directly via DPO@firebirdltd.co.uk

4.3.4 The DPO is supported in their role by a College employee, this person is known as the DPO's Data Protection Link Officer. All enquiries, complaints, requests and suspected breaches of security, should be referred to the Data Protection Link Officer in the first instance, who will then notify the DPO.

4.3.5 The College's Data Protection Link Officer is Jo Liddle and can be contacted at jliddle@sidmouthcollege.devon.sch.uk.

4.4 Employees, temporary staff, contractors, visitors

4.4.1 All employees, temporary staff, contractors, visitors and other individuals processing personal data on behalf of the College, are responsible for complying with the contents of this policy.

4.4.2 All individuals shall remain subject to the common law duty of confidentiality when their employment or relationship with the College ends. This does not affect an individual's rights in relation to whistleblowing.

4.4.3 Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.

5 Policy content

5.1 Data Protection Principles

5.1.1 The GDPR provides a set of principles which govern how the College handles personal data. In summary, these principles state that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary for the purpose it was processed
- accurate and where necessary kept up to date
- kept for no longer than is necessary
- processed in a manner that ensures appropriate security of the data

5.1.2 The College and all individuals processing personal data controlled by the College, shall comply with the data protection principles in the following manner:

5.2 Lawfulness, fairness and transparency

5.2.1 *Lawful processing*

5.2.2 Personal data will only be processed where there is a lawful basis for doing so. This will be where at least one of the following applies:

- The data subject has given consent
- It is necessary for the performance of a contract or entering into a contract with the data subject
- It is necessary for compliance with a legal obligation
- It is necessary to protect the vital interests of a person
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official duties

5.2.3 When special categories of personal data are processed (i.e. data which reveals a person's racial or ethnic data; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data (e.g. fingerprints); health data; sex life or sexual orientation), this shall only be done where a lawful basis has been identified from the list above, and one from the following list:

- The data subject has given explicit consent
- The processing is necessary for the purposes of exercising or performing any right or obligation which is imposed on the College in relation to employment, social security and social protection law (e.g. safeguarding individuals at risk; protection against unlawful acts; prevention against fraud)
- It is necessary to protect the vital interests of any person where the data subject is physically or legally incapable of giving consent
- The processing is necessary for the establishment, exercise or defence of legal claims
- The processing is necessary in the substantial public interest
- The processing is necessary for the assessment of the working capacity of the employee

5.2.4 *Consent*

5.2.5 Most of the College's processing of personal data will not require consent from data subjects (or their parents/carers as appropriate), as the College needs to process this data in order to carry out its official tasks and public duties as a College.

5.2.6 However, there are circumstances when the College is required to obtain consent to process personal data, for example:

- To collect and use biometric information (such as fingerprints)
- To send direct marketing or fundraising information by email or text
- To take and use photographs, digital or video images and displaying, publishing or sharing these in a public arena such as:
    - on social media;
    - in the College prospectus;
    - on the College website;
    - in the press/ media;
    - in the College newsletter

5.2.7 When the College relies on consent as its lawful basis, it shall ensure the person providing it has positively opted-in to the proposed activity and is fully informed as to what they are consenting to and any non-obvious consequences of giving or refusing that consent. Consent shall not be assumed as being given if no response has been received e.g. a consent form has not been returned. Where consent is being obtained for the collection or use of children's information, consent shall be obtained from a parent or guardian until the child reaches the age of 12. Consent shall be obtained directly from children aged 13 years and over, where those children are deemed by the College to have sufficient maturity to make the decision themselves (except where this is not in the best interests of the child. In such cases, consent will be obtained from an adult with parental responsibility for that child).

5.2.8 The College shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing. All forms requesting consent shall include a statement informing the person of their right to withdraw, and an email address so they may notify the College of any changes or withdrawal of consent.

5.2.9 *Fairness and transparency*

5.2.10 The College shall be fair, open and transparent in the way it handles personal data, and will publish privacy notices which explain:

- What personal data the College processes and why
- What our lawful basis is when we process that data
- Who we might share that data with
- If we intend to transfer the data abroad
- How long we keep the data for
- What rights data subjects have in relation to their data
- Who our Data Protection Officer is and how to contact them

5.2.11 The College's privacy notices shall be clear, concise, easily accessible and published on the College's website Sidmouth College - GDPR Information - SIDMOUTH COLLEGE All forms collecting personal data shall include reference to the College's privacy notices and a link provided to their location.

5.3 Purpose limitation

5.3.1 The College shall collect personal data for specified (i.e. as described in the College's privacy notices), explicit and legitimate purposes and shall not process this data in any way would could be considered incompatible with those purposes (e.g. using the data for a different and unexpected purpose).

5.4 Data minimisation

5.4.1 The College shall ensure the personal data it processes is adequate, relevant and limited to what is necessary for the purpose(s) it was collected for.

5.5 Accuracy of data

5.5.1 The College shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date. Where personal data is found to be inaccurate, this information will be corrected or erased without delay.

5.5.2 The College will send frequent reminders, on at least an annual basis, to parents/carers, students and employees, to remind them to notify the College of any changes to their contact details or other information.

5.5.3 The College shall carry out periodic sample checks of pupil and employee files containing personal data, to ensure the data is accurate and up to date.

5.6 Storage limitation and disposal of data

5.6.1 The College shall keep personal data for no longer than is necessary for the purpose(s) of the processing. The College shall maintain and follow a Record Retention Schedule, which sets out the timeframes for retaining personal data. This schedule shall be published alongside the College's privacy notices on the website.

5.6.2 The College shall designate responsibility for record disposal/deletion to nominated employees, who shall adhere to the College's Record Retention Schedule and ensure the timely and secure disposal of the data.

5.7 Security of personal data

5.7.1 The College shall have appropriate security in place to protect personal data against unauthorised or accidental access, disclosure, loss, destruction or damage. This will be achieved by implementing appropriate technical and organisational security measures.

5.8 Technical security measures

5.8.1 The College shall implement proportionate security measures to protect its network and equipment and the data they contain. This includes, but is not limited to:

- having a Firewall, anti-virus and anti-malware software in place
- applying security patches promptly
- restricting access to systems on a 'need to know' basis
- enforcing strong password policies; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others
- encrypting laptops, USB/memory sticks and other portable devices or removable media containing personal data
- regularly backing up data
- regularly testing the College's disaster recovery and business continuity plans, to ensure data can be restored in a timely manner in the event of an incident

5.9 Organisational security measures

5.9.1 The College will ensure the following additional measures are also in place to protect personal data:

- Employees shall sign confidentiality clauses as part of their employment contract
- Data protection awareness training shall be provided to employees during induction and annually thereafter
- Policies and guidance shall be in place relating to the handling of personal data whilst during and outside of College. These will be communicated to employees and other individuals as necessary, including policy revisions. A policy declaration shall be signed by employees and retained on their personnel file.
- Data protection compliance shall be a regular agenda item in governing body and Senior Leadership Team meetings.
- Cross cutting shredders and/or confidential waste containers will be available on the College's premises and used to dispose of paperwork containing personal data.
- Appropriate equipment and guidance will be available for employees to use and follow when carrying paperwork off College premises.
- The College's buildings, offices and where appropriate classrooms, shall be locked when not in use.
- Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need to know basis.
- Procedures shall be in place for visitors coming onto the College's premises. These will include signing in and out at reception, wearing a visitor's badge and being escorted by a College employee (unless the visitor holds a valid Disclosure and Barring Service certificate, or it is otherwise appropriate for the person not to be escorted).
- The College shall have procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident.

5.10 Rights of Data subjects

5.10.1 Data subjects have several rights under the data protection legislation. The College shall comply with all valid requests (written or verbal) from data subjects exercising their rights without delay, and within one month at the latest.

5.10.2 Data subjects have the right to:

- Be informed about the use, sharing and storage of their data (this is a privacy notice)
- Request access to the personal data the College holds about them (this is a subject access request)
- If their data is inaccurate or incomplete they can request that it is corrected
- Ask for their data to be deleted when it is no longer needed
- Restrict the use of their data in certain circumstances

- Port (transfer) their data to another organisation in certain circumstances
- Object to the use of their data in certain circumstances (this includes direct marketing)
- Prevent automated decisions being taken about them (including profiling)
- Raise a concern with the College about the handling of their personal data. If they remain dissatisfied with College's response, they have the right to escalate this to the Information Commissioner's Office.

5.11 Handling requests

5.11.1 Data subjects exercising their rights are recommended to put their request in writing and send it to the College at Primley Road, Sidmouth, EX10 9LG or enquiries@sidmouthcollege.devon.sch.uk Data subjects can also exercise their rights verbally. Requests shall be handled in line with the College's Data Protection Request Handling Procedure.

5.12 Data protection by design and default

5.12.1 The College shall have appropriate technical and organisational measures in place which are designed to implement the data protection principles in an effective manner, and will ensure that by default, it will only process personal data where it is necessary to do so. The College's Data Protection Policy and supplementary policies, procedures and guides, explain how the College aims to achieve this.

5.13 Joint controller agreements

5.13.1 The College shall sign up to agreements with other data controllers where personal data is shared or otherwise processed on a regular basis, where it is necessary to do so.

5.14 Data processors

5.14.1 The College shall carry out checks with prospective data processors (e.g. suppliers providing goods or services which involve the processing of personal data on the College's behalf) to assess they have appropriate technical and organisational measures that are sufficient to implement the requirements of the data protection legislation and to protect the rights of data subjects.

5.14.2 The College's Data Protection Officer, IT Manager and Data Protection Link Officer shall assess the appropriateness of data processors before the College purchases their services. A record will be kept of their findings on a Data Processor Due Diligence Report.

5.14.3 The College shall ensure there are appropriate written contracts/Terms of Service in place with data processors, which contain the relevant clauses listed in Article 28 of the GDPR.

5.15 Record of processing activities

5.15.1 The College shall maintain a record of its processing activities in line with Article 30 of the GDPR. This inventory shall contain the following information:

- Name and contact details of the College and its Data Protection Officer

- Description of the personal data being processed
- Categories of data subjects
- Purposes of the processing and any recipients of the data
- Information regarding any overseas data transfers and the safeguards around this
- Retention period for holding the data
- General description of the security in place to protect the data

5.15.2 This inventory shall be made available to the Information Commissioner upon request.

5.16 Management of personal data breaches

5.16.1 The College shall have procedures in place to identify, report, record, investigate and manage personal data breaches (i.e. security incidents involving personal data). These include security incidents resulting in the:

- unauthorised or accidental disclosure or access to personal data
- unauthorised or accidental alteration of personal data
- accidental or unauthorised loss of access or destruction of personal data

5.16.2 All security incidents and suspected personal data breaches must be reported to the Data Protection Officer immediately, via the College's Data Protection Link Officer, by emailing dpo@sidmouthcollege.devon.sch.uk or telephone 01395 514823.

5.16.3 All incidents will be recorded in the College's data breach log and investigated by a member of the Senior Leadership Team (or other person as appropriate), under the support and direction of the College's Data Protection Officer.

5.16.4 *Notification to the ICO and Data Subjects*

5.16.5 The Data Protection Officer shall determine whether the College must notify the Information Commissioner's Office and data subjects.

5.16.6 Where a breach is likely to result in a risk to the data subject, for example if they could suffer damage, discrimination, disadvantage or distress as a result of the breach, the College (or the Data Protection Officer) shall notify the Information Commissioner's Office (ICO) within 72hrs of becoming aware of the breach.

5.16.7 If the breach is likely to result in 'high risks' to data subjects, for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm, the College shall inform the data subject promptly and without delay.

5.16.8 When informing a data subject of a personal data breach involving their personal data, the College shall provide in clear, plain language the:

- nature of the incident

- name and contact details of the Data Protection Officer
- likely consequences of the breach
- actions taken so far to mitigate possible adverse effects

5.17 Data Protection Impact Assessments

5.17.1 The College shall carry out Data Protection Impact Assessments (DPIAs) on all processing of personal data, where this is likely to result in high risks to the rights and freedoms of data subjects, particularly when using new technologies. This includes, but is not limited to the following activities:

- Installing and using Closed Circuit Television (CCTV)
- Collecting and using biometric information, such as fingerprints
- Sharing personal data or special category data with other organisations
- Using mobile Apps to collect or store personal data, particularly about children
- Storing special category data in the 'Cloud'
- Using systems that record large volumes of personal data, particularly where data processors are involved

5.17.2 The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA, to ensure the mitigations are put in place.

5.18 Appointment of a Data Protection Officer

5.18.1 The College shall appoint a Data Protection Officer to oversea the processing of personal data within the College, in compliance with Articles 37-38 of the GDPR. This person shall be designated on the basis of professional qualities and in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of the GDPR.

5.18.2 The College shall publish the contact details of the Data Protection Officer and communicate these to the Information Commissioner's Office.

6 Policy history

Policy Version and Date	Summary of Change	Amended by	Implementation Date
Version 1.2 July 2020	• 5.2.3 – amended to read: *When special categories of personal data are processed (i.e. data which reveals a person's racial or ethnic data; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data (e.g. fingerprints); health data; sex life or sexual orientation), this shall only be done where a lawful basis has been identified from the list above, and one from the following list…* • 5.2.11 – amended to read: *The College's privacy notices shall be clear, concise, easily accessible and published on the College's website. All forms collecting personal data shall include reference to the College's privacy notices and a link provided to their location.* • The following paragraphs have been removed: 5.2.12; 5.2.13; 5.2.14 • 5.5.3 – amended to read: *The College shall carry out periodic sample checks of pupil and employee files containing personal data, to ensure the data is accurate and up to date.* • 5.10.1 – amended to read: *Data subjects have several rights under the data protection legislation. The College shall comply with all valid requests (written or verbal) from data subjects exercising their rights without delay, and within one month at the latest.* • 5.10.2 – bullet points have been re-worded in full	Amber Badley, Data Protection Officer	1 July 2020

	• 5.11.1 – amended to read: *Data subjects exercising their rights are recommended to put their request in writing and send it to the College at [insert College postal address and email address]. Data subjects can also exercise their rights verbally. Requests shall be handled in line with the College's Data Protection Request Handling Procedure.* • The following paragraphs have been removed: 5.11.2; 5.11.3; 5.11.4; 5.11.5; 5.11.6; 5.11.7; 5.11.8 • 5.14.2 has been amended to read: *The College's Data Protection Officer, IT Manager and Data Protection Link Officer shall assess the appropriateness of data processors before the College purchases their services. A record will be kept of their findings on a Data Processor Due Diligence Report.*		
Version 1.1 1 July 2019	• Version number and policy date (page 1) • 2.2 amended to read *[insert relevant policies and procedures such as the E-Safety Policy; ICT Policy etc].* • 4.2 amended to read: *Headteacher [or Principal]* • 4.2.1 amended to read: *The Headteacher [or principal]* • 4.3.3 amended to read: *The DPO is Amber Badley, who can be contacted through the College at [insert College email address] or directly via DPO@firebirdltd.co.uk* • 5.2.7 amended to include: *Where consent is being obtained for the collection or use of children's information, consent shall be obtained from a parent or guardian until the*		

	child reaches the age of 12. Consent shall be obtained directly from children aged 13 years and over, where those children are deemed by the College to have sufficient maturity to make the decision themselves (except where this is not in the best interests of the child. In such cases, consent will be obtained from an adult with parental responsibility for that child). • 5.2.12 amended to read: *This notice will be published on the College's website; parents will be directed to this on an annual basis.* • 5.2.13 amended to read: *Employees will be given a privacy notice explaining how the College handles employee information when they join the College and directed to this annually thereafter.* • 5.11.1 amended to read: *Data subjects exercising their rights are recommended to put their request in writing and send it to the College at [insert College postal address and email address]. Data subjects can also exercise their rights verbally. In such cases, the College will promptly write to the data subject outlining the verbal discussion/request and will ask the data subject to confirm this is accurate.* • Renumbering of paragraphs in section 5.11-5.12		

	• 5.11.4 amended to read: *Students can request access to their own personal data when they have sufficient maturity to understand their rights; know what it means to make such a request and can interpret the information they receive. The Information Commissioner's Office and the Department for Education guidance, suggests that children aged 13 years and above, may have sufficient maturity in these situations, however it is for the College to decide this on a case by case basis.*		
Version 1.0 25 May 2018	This policy replaces the College's existing Data Protection Policy	Amber Badley, Data Protection Officer	25 May 2018

Declaration

I confirm that I have read, understood and shall adhere to Sidmouth College's Data Protection Policy Version 1.2, dated 20th July 2020 and the supporting policies and procedures referred to in this policy.

Name:	
Job title:	
Date:	
Signature:	

Instructions for College admin

This declaration must be kept in an easily retrieval file. In the case of an employee, this should be kept on their personnel file.

Appendix 1

Data Protection Policy Definitions

Term Used	Summary Definition
Personal data	Personal data means any information relating to an identified or identifiable living individual. This includes a name, identification number, location data, an online identifier, information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Special categories of personal data	Special categories of personal data mean personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs and the trade union membership of the data subject. It also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, and data relating to an individual's sex life or sexual orientation.
Processing	Processing means any operation or set of operations which is performed on personal data, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data subject	An identifiable, living individual who is the subject of personal data.
Data controller	A data controller is an organisation who determines the purposes and means of the processing of personal data.
Data processor	A data processor is an organisation who processes personal data on behalf of a data controller, on their instruction.