MILTON ABBEY SCHOOL

DATA PROTECTION POLICY (Incorporating Website Cookie Guidance)	
Issue Date:	September 2024
Review Date:	September 2025
Policy Contact:	Steve Lane
Approved by:	James Watson

This policy (together with any other documents referred to in it) sets out the basis on which we process personal data that has been provided to or collected by The Council of Milton Abbey School Limited ("the School"). Please read the following carefully to understand the School's views and practices regarding personal data and its treatment. By visiting www.miltonabbey.co.uk the user accepts and consents to the practices described in this policy.

Introduction

The School may need to process personal data about its current, prospective and former pupils and their parents, its current, prospective and former staff, its suppliers/contractors, its current and prospective supporters and other individuals connected to the School, as part of its everyday operations and is legally obliged to process such personal data in accordance with the Data Protection Act 2018 ("the DPA") and the UK General Data Protection Regulations (GDPR).

Following the UK leaving the EU, the principles of the EU GDPR were adopted as the UK GDPR, and in June 2021, the EU approved adequacy decisions for the UK law to be considered "essentially equivalent" to EU legislation, which means data can continue to flow freely between the two areas, in the majority of circumstances. This decision is expected to last until June 2025.

The School is the data controller of this personal data under the DPA. The School is committed to compliance with the DPA and GDPR and takes seriously the responsibility of handling personal information.

This policy has been developed to ensure that the School meets its obligations under these laws.

The data protection principles contained in the DPA ("the Data Protection Principles") require the School to ensure all personal data is:

- accurate and up to date;
- adequate, relevant and not excessive;
- collected for specified, explicit, and legitimate purposes;
- fairly and lawfully processed;
- kept for no longer than is necessary (in line with the School's Data Retention Schedule);
- processed in a secure manner

In addition the DPA requires that personal data is:

- not transferred to other countries without adequate protection
- protected by appropriate security;
- processed in accordance with the data subject's rights;

Key Data Protection Staff

1. James Watson, as Headmaster, is the School's Senior Information Risk Owner (SIRO). The SIRO has responsibility for implementing and managing information risks within the organisation. They have oversight of information risks within the organisation and will inform and advise the wider staff body and Governing Body on how to mitigate any information risks.

2. Chris Barnes, as Senior Deputy Head is responsible for all pupil related data held by Milton Abbey School.

3. Tracey Edwards, as the Head of Operations is responsible for all 'adult'

4. Steve Lane is the School's Data Protection Compliance Lead (DPCL).

The Data Protection Compliance Lead is responsible for:

- arranging appropriate training for members of the School's staff who are responsible for processing personal data, ensuring requirements are explained at part of the induction process for new staff and advising staff responding to Subject Access Requests;
- endeavouring to ensure that personal data is processed by the School in compliance with this policy and the Data Protection Principles;
- the enforcement, monitoring and review of this policy

Personal Data Processed By The School

Personal data processed by the School may be information stored electronically or in paper- based filing systems and can take different forms including factual information, expressions of opinion, images or other recorded information relating to a living individual who can be identified.

Personal data processed by the School may include:

- additional information required for the employment or appointment of staff and contractors including images and biometric data
- any education related records or information including academic, disciplinary, admissions and attendance records (including information about any special needs); examination scripts and marks of pupils;
- employment details and financial information relating to parents and guardians;
- images of pupils, including photographs of pupils engaging in School activities;
- names, addresses, email address and other contact details;
- references given or received by the School about pupils or staff;

Sensitive personal data processed by the School about an individual may include data concerning their ethnic group, religious beliefs, criminal records and proceedings, trade union membership and relevant medical information.

The School may collect personal data directly from the data subject (or in the case of a pupil, from his/her parents or guardians) and from third parties (for example, other schools, authorities).

You may also give us information about you by filling in forms on our website www.miltonabbey.co.uk or by corresponding with us by phone, email or otherwise. This includes information you provide when you register details on our website, subscribe to any online services used by the school, interact with the School's accounts on social media platforms on our site, enter a competition or survey and when you report a problem with our site. The information you give us may include your name, address, email address and phone number, financial and credit card information, personal description and photograph.

Why Do We Process Personal Data?

Personal data (including sensitive personal data, where appropriate) is, and will be, processed by the School in accordance with the Data Protection Act for the following purposes:

The provision of education and support to the pupils, including: activities in connection with the admissions process; participation of pupils in internal and public examinations and the publication of results and the pupils' individual achievements; the monitoring of and reporting on pupils' educational development including the preparation of individual performance reports and letters to parents; facilitating participation in and the provision of extra-curricular activities, such as the Combined Cadet Force and Department of Education schemes; the provision of bursaries to pupils; careers services including the provision of references to current and former pupils; and the provision of alumni events and services by the Milton Abbey Association;

The general administration of the School including: the provision of information to relevant school authorities for the purpose of monitoring the School's performance; the preparation of annual returns and reports to be submitted to educational monitoring organisations and inspectorates;

The promotion of the School and its objectives, including: the use of photographic images of pupils on the School's website as well as in hard copy promotional or marketing material published by the School (NB: pupil and parent consent is sought as part of the admissions process before imagery is used in this way), including but not limited to monthly e-newsletters, termly newsletters circulated to current, former and prospective parents, members of the Milton Abbey Association, business contacts, associates and other contacts or prospective associates of the School and the general public;

The administration of the School's staff, agents and suppliers including: DBS checks; the provision of references for current and former staff; disciplinary and grievance procedures and general appraisal purposes; and

The fulfilment of the School's contractual and legal obligations.

Processing Of Personal Data

The School will only process personal data for the purpose(s) for which it was originally acquired and will not process it for any other purpose without the data subject's permission, unless required or otherwise permitted by law.

The School will not transfer personal data outside of the EEA, unless it is satisfied that the data subject's rights under the DPA will be adequately protected.

The School will seek permission from an individual and, in the case of a pupil, their parents or guardians before allowing that person to feature particularly prominently in films, articles or other materials produced by, or otherwise prepared in assistance with, the School and published for documentary, marketing or promotional purposes.

When processing personal data for the purposes set out above the School may communicate by post, email and SMS.

All staff have a responsibility to handle personal data they come into contact with fairly, lawfully, responsibly and securely and in accordance with their Employment Manual and all relevant School policies and procedures. Responsible processing extends to the creation and generation of new personal data.

Response To Personal Data Breaches

A “personal data breach” means 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 other words: any event or incident which compromises the confidentiality, integrity or availability of personal data.

Examples of personal data breaches can include, but are not limited to:

- Access to documentation not stored securely by third parties
- Alteration of personal data without permission;
- Computing devices containing personal data being lost or stolen;
- Cyber attacks
- Electronic access by an unauthorised third party (including hacking);
- Deliberate or accidental action (or inaction) by a controller (the school) or processor (staff or contractors);
- Loss of availability of personal data (e.g. equipment failure or network outage);
- Sending personal data to an incorrect recipient;

All staff must report any breach of personal data to the Data Protection Compliance Lead, who will assess any actual or potential impact of the breach. The Data Compliance Lead will report certain types of personal data breach (those which risk an impact to individuals, including when those individuals cannot be contacted) to the ICO within 72 hours. Further detail is outlined in Annex A.

If staff are in any doubt as to whether or not they should report something, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision.

In most cases of accidental, non-negligent data breach, the School will not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the school, and for those affected, so non-reporting could itself be a disciplinary matter.

The Data Protection Compliance Lead must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms.

The School will keep a record of any personal data breaches and mitigating actions taken, regardless of whether we need to notify the ICO or the subject of the personal data.

Third Parties With Whom The School May Need To Share Personal Data

Personal data shall only be disclosed to those members of the School's staff, agents and suppliers who need to access the personal data to carry out the purpose(s) for which it was acquired. The School adopts appropriate security measures to ensure that personal data is kept secure and not processed without proper authority. The School observes legislative requirements and current best practice to ensure personal data is kept for no longer than necessary.

From time to time the School may pass personal data (including sensitive personal data where appropriate) to third parties, including local authorities, other public bodies (e.g. the DBS, the NHS, Department for Education, and Department for Work and Pensions), independent school bodies such as the Independent Schools Inspectorate and the Independent Schools Council, health professionals, the School's professional advisers and its subsidiaries, who will process the data for the purposes set out in section 5 of this policy or where otherwise required by law.

The School may also, unless the data subject requests otherwise, share personal data about former pupils with the Milton Abbey Association who may contact alumni from time to time regarding the School and its activities, and for promotional and marketing purposes.

Rights Of Access To Personal Data

Data subjects have the right to be given access to personal data held about them by any data controller this information could be kept on physical or electronic file, CCTV, social media post, emails, or within archives. This is enabled through a process called a Data Subject Access Request (DSAR).

By law, people can ask you for a copy of any information that's to do with them. It might be saved on your system, but if it's about them, it's their personal data, and they have a right to see it in writing, they have made a subject access request (DSAR), And you need to take action.

The Information Commissioner's Office's guidance is that, in the majority of cases, by the age of 13 an individual has sufficient maturity to understand their rights, make their own decisions in relation to privacy, and to make an access request themselves if they wish. Therefore, in relation to a DSAR for information relating to a pupil, the pupil can initiate a request and the pupil will be informed if such a request is made by a parent or guardian. A parent or guardian would normally be expected to make a request on a child's behalf if the child is less than 12 years old.

If individuals wish to access their personal data held by the School, then a request should be submitted to the Safeguarding Team in relation to information about pupils, or the Head of Operations in relation to information about adults. If the School are not sure the requester is who they say they are, the school must check this quickly. The school. Shouldn't. Ask for formal ID. Unless it's necessary and proportionate. Instead, you could ask questions that only they would know, about reference numbers or appointment details for example. Or you can ask for ID that you can actually verify. There's little point insisting on photo ID if you don't know what the requester looks like - it should be proportionate.

If the SAR Is made by someone other than the person the data is about (such as a friend, relative or solicitor), check their allowed to have it. You will need to see that they have written authority to act on behalf of the person concerned, or a document showing general power of attorney (This includes children 12 years or over).

The School will respond to such Subject Access Requests within the statutory timeframe of one month of receipt, unless an exemption from the right of access under the DPA applies. Common exemptions to disclosure include information that is legally privileged or that would directly or indirectly lead to disclosing information about another individual.

You've got one calendar month to get what you need together and send it to the relevant person. If you need to check their ID or ask for other information, you can wait until they reply before starting the clock on your one month time limit. But you should ask for any additional information you need as soon as possible.
There are three important things to know about. The one calendar month time frame: It doesn't matter if the day you receive the request isn't a working day. For example, if you receive a request on Saturday 7 of March, you should respond by Tuesday 7 April.

If the source. Due date. Falls on a weekend or public holiday, You have until the next working day to respond. For example, if you receive a request on 25 November You should respond by 27 December.

You can't add extra days when the calendar month is shorter. For example, if you receive a request on the 31 January, you should respond by the 28 February.

Top tip: You could set reminders to complete your s within 28 days That way you'll always be on time, regardless of the month.

If its a very complex request, or if the request has made a lot of requests, you can take an extra 2 calendar months to respond. But you must let the requester know there will be a delay before the end of the first calendar month.

The Information Commissioner's Office advises that Subject Action Requests should be focused, clear in their purpose, and not 'vexatious, unfounded or excessive'. Organisations can be exempted from responding if requests are not clear and specific, such that they would require an unreasonable amount of time to response to.

Before you, consider giving the requester their information, look through it carefully to make sure it really is their information.

For example, if you have an e-mail that mentions a number of different people, you should `redact' (black out) any information which **doesn't** relate to the person making the SAR. This is important, because most of the time you would avoid disclosing information about other people. Another way of doing this is to copy and paste sections relevant to the SAR into a separate document and send them that instead.

If you are using a computer to redact information, make sure you get advice on how to save it as a new file. Otherwise, there's a risk that someone could delete your blacked-out sections and read the text underneath.

Appendix A explains in further detail how Data Subject Access Requests (DSARs) will be managed by the School.

The vast majority of Subject Access Requests receive a timely and satisfactory response, but if you receive an unsatisfactory response, please escalate your concern as follows:

- By complaint in writing to the Chair of Governors.
- By external complaint to the Information Commissioner's Office.
- By requesting further information/clarification from the staff member responding.

The School will endeavour to ensure that all personal data held in relation to individuals is accurate and up to date. Individuals must notify the School of any changes to information held about them and can request that inaccurate information about them is corrected.

The School will take reasonable steps to ensure that personal data is kept secure and is only accessed by authorised members of its staff for the purposes for which it is held. All staff will be made aware of this data protection policy and their duties under the DPA.

Use Of The School's Website

By visiting www.miltonabbey.co.uk you are accepting and consenting to the practices described in this policy.

With regard to each of your visits to our site we may automatically collect the following information:

- information about your visit, including the full Uniform Resource Locators (URL) clickstream to, through and from our site (including date and time); products you viewed or searched for; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page and any phone number used to call our customer service number.
- technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform;

Information we collect about you when you use our website. We will use this information:

- as part of our efforts to keep our site safe and secure.
- to administer our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- to allow our site to deliver customised content and advertising to users whose activity indicates that they are interested in a particular subject;
- to allow you to participate in interactive features of our service, when you choose to do so;
- to improve our site to ensure that content is presented in the most effective manner for you and for your computer;

Whilst using our website, we may also collect certain personally identifiable information, including email address, name, home or work address or telephone number. Any such data will be processed in accordance with this policy. Please note that any personal or sensitive personal data that you disclose through public message boards can be accessed and collect by third parties.

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Website Cookie Guidance

This section explains how we use cookies and similar technologies on our website. By using our website, you consent to the use of cookies as described in this policy.

Cookies are small text files that are placed on your device (computer, tablet, smartphone, etc.) when you visit a website. They help the website recognise your device and remember certain information about your visit. Cookies serve various purposes, such as enabling website functionality, improving user experience, and providing analytics.

We use cookies for the following purposes:

- **Analytical Cookies:** We use analytical cookies to collect information about how visitors use our website. These cookies help us understand which pages are most popular, the duration of visits, and other relevant statistics. This data is anonymous and aggregated, enabling us to improve the website's performance and user experience.
- **Essential Cookies:** These cookies are necesDSARy for the basic functioning of our website. They enable you to navigate the site and access essential features, such as secure areas and online forms. Without these cookies, the website may not function correctly.
- **Functionality Cookies:** These cookies remember your preferences and choices while using our website. They help personalize your experience and provide enhanced functionality, such as remembering your language preferences or customizations.
- **Performance Cookies:** Performance cookies help us track the performance of our website and identify any issues that may arise. They allow us to improve the site's speed and overall performance.

Some of our website's features may be provided by third-party services or platforms. These third parties may also use cookies on our site for the purposes described in their respective privacy and cookie policies. We do not have control over these cookies, and you should review the relevant third-party policies for more information.

You can control and manage cookies through your browser settings. Most browsers allow you to block or delete cookies, and you can also set preferences for specific websites. However, please note that blocking or disabling certain cookies may affect the functionality and user experience of our website.

Any queries about this policy or how personal data is processed by the School should be referred to the Data Protection Compliance Lead for further guidance.

Enforcement And Contact Information

If an individual believes that the School has not complied with this policy or has acted otherwise than in accordance with the DPA, the individual should notify the Data Protection Compliance Lead who shall, where appropriate, refer the matter for resolution in accordance with the School's grievance/ disciplinary procedure (for staff) or complaints procedure (for parents/pupils).

This policy applies to all staff of the School and breach of the policy may result in appropriate disciplinary action being taken.

Appendices have been removed from this version