



Data Protection Policy

Review cycle:	Every 3 years
Review by:	SMT, G(F&GP)
Last Governor Approval:	Summer 2018
Next Governor Approval:	Summer 2021

Policies linked to:

- Recruitment Policy
- Assessment Recording and Reporting Policy
- Admissions Policy
- Attendance Register (registration of pupils) Policy
- First Aid and Medicines Policy and Procedure
- Critical Incident Plan
- Information and Records Retention Policy

This document also appears on:

- School Website
- Staff Intranet

Introduction

This policy is intended to provide information about how the School will use (or "process") personal data, regardless of whether it is in paper or electronic format.

The School aims to ensure that all personal data collected about staff, pupils, parents, governors, contractors, volunteers, visitors and other individuals is collected, stored and processed in accordance with current data protection legislation.

It applies in addition to the School's terms and conditions, and any other information the School may provide about a particular use of personal data, including e.g. the School's policy on taking, storing and using images of children. The School's Privacy Notice for Pupils should be read and discussed by families so that pupils have an understanding of the principles by which the School processes their data.

Anyone who works for, or acts on behalf of, the School (including staff, volunteers, governors and service providers) should also be aware of and comply with the School's Privacy Notice for Staff, which also provides further information about how personal data about those individuals will be used.

Responsibility for Data Protection

In accordance with legislation, the School has notified the Information Commissioner's Office of its processing activities. The School's ICO registration number is Z8472625 and its registered address is 15 Amersham Road, Amersham, Buckinghamshire HP6 5PF.

The Governing Body has overall responsibility for ensuring that the School complies with legislative regulations.

The School has appointed the Director of Finance and Operations to take primary responsibility for Data Protection on behalf of the Data Controller, and will endeavour to ensure that all personal data is processed in compliance with this policy, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

All staff may only process data in order to fulfil their day-to-day roles and as such, have a responsibility for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the School of any changes to their personal data.
- Contacting the Director of Finance and Operations in the event of any data processing activity which falls outside of the purposes detailed below, including those which may require additional consent or in the event of a data breach.
- Conducting Privacy Impact Assessments when engaging in a new activity which may significantly affect the privacy rights of a data subject.

Data Protection Principles

The School's policy is that personal data shall be:

- Fairly and lawfully processed in a transparent manner
- Processed for limited, legitimate and specific purposes
- Adequate, relevant and not excessive

- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Kept secure
- Processed in accordance with GDPR guidelines on transferral of data outside of the European Economic Area (EEA)

Data Processing

The School is entitled to process relevant personal data regarding pupils and their parents and guardians as part of its operation and shall take all reasonable steps to do so in accordance with this policy.

Processing may include collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying and sharing. Processing can be automated or manual.

The School is registered to process personal data for the following purposes:

- The provision of education as a primary function
- Educational support and ancillary purposes
- Staff administration
- Advertising, marketing and public relations
- Staff, agent and contractor information
- School administration

Personal data processed by the School may include (but is not limited to):

- Personal details such as home address, contact details, date of birth and next of kin
- Identification documents
- Pupils' performance at School, including assessments, reports, examination reports, discipline record, attendance information
- Special educational needs
- Medical records and information, including details of any illnesses, allergies or other medical conditions suffered by a child
- Safeguarding information
- Details of any support received, including learning support, therapists, counselling, care plans and support providers
- Sensitive personal data such as ethnic group, religious beliefs
- Images of pupils and staff (and occasionally other individuals) engaging in School activities
- Bank details and National Insurance Number
- Performance Development Records
- CCTV images for security purposes

Where sensitive personal data is processed by the School, the explicit consent of the appropriate individual will generally be sought in writing.

Use of Personal Data by the School

The School has an Information and Records Retention Policy (updated April 2018) which demonstrates the manner in which data is held, secured and erased from our systems.

Certain data is exempt from the right of access under the Data Protection Act. This may include information that identifies other individuals, information that the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination or test answer scripts. Other data, such as the following, are also exempted from the provisions of the Data Protection Act:

- the prevention or detection of crime
- the assessment of any tax or duty
- where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School
- photographs taken by parents, guardians and friends at School events that are purely for personal use and not public display

These examples are only some of the exemptions under the Act. Any further information on exemptions should be sought from the Director of Finance and Operations.

Consent may be required for the processing of personal data unless the processing is necessary for the School to undertake its obligations to pupils and their parents or guardians. Any information that falls under the definition of personal data, and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this policy.

Within the requirements of this policy, the following have specific responsibility unless an exemption exists:

	Creation of personal data	Retention of personal data	Destruction of personal data
Headmaster (including PA/Registrar)	Correspondence relating to pupils and parents. Staff records. Prospective pupil enquiry data. Staff contact lists.	Correspondence relating to pupils and parents. Staff records. Staff contact lists.	Correspondence relating to pupils and parents. Staff records. Staff contact lists.

Director of Finance and Operations	Correspondence relating to pupils and parents. Billing ledger. Purchase ledger. Staff records, including payroll and salaries.	Correspondence relating to pupils and parents. Billing ledger. Purchase ledger. Staff records, including payroll and salaries.	Correspondence relating to pupils and parents. Billing ledger. Purchase ledger. Staff records, including payroll and salaries.
Senior Master (including School Secretaries and Medical Centre staff)	Pupil records. Parent records. Medical data.	Pupil records. Parent records. Medical data.	Pupil records. Parent records. Medical data.
Deputy Head (Academic)	Pupil academic records and data.	Pupil academic records and data.	Pupil academic records and data.
Head of Middle School	Pupil academic records and data.	Pupil academic records and data.	Pupil academic records and data.
Head of Lower School	Pupil academic records and data.	Pupil academic records and data.	Pupil academic records and data.
Head of Pre-Prep	Pupil academic records and data.	Pupil academic records and data.	Pupil academic records and data.
Heads of Department	Pupil academic records and data.	Pupil academic records and data.	Pupil academic records and data.
Counsellor	Pupil and staff personal data.	Pupil and staff personal data.	Pupil and staff personal data.
Caterer	Pupil and staff food allergies and nutritional data.	Pupil and staff food allergies and nutritional data.	Pupil and staff food allergies and nutritional data.

All members of staff and the governors are provided with regular training on compliance of the requirements of the Data Protection Act.

Data Accuracy and Security

At The Beacon, data security is by design and our electronic and paper systems are built to ensure that security is paramount.

The School will endeavour to ensure that all personal information held in relation to an individual is accurate. Individuals must notify the School of any changes to information held about them,

including contact details and Next of Kin information. Individuals have the right to request that inaccurate information about them is erased or corrected. Individuals have the right for their data to be removed when no longer used by the School.

The School will take reasonable steps to ensure that members of staff will only have access to personal data that relates to their area of responsibility in respect of data on pupils, their parents or guardians, and staff on a “need to know” basis. All staff will be made aware of this policy and their duties under GDPR. The School will ensure that all personal information is held securely and is not accessible to unauthorised persons. Personal data must be protected by physical means (locked cabinets or locked rooms/offices) or through the use of electronic data protection. Personal data is not to be removed from the School site without the express permission of the Director of Finance and Operations.

Measures are in place to show that we have integrated data protection into all of our data processing activities, including:

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles
- Completing Privacy Impact Assessments where the School’s processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- Integrating data protection guidance and policy 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; we will also keep records of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular, paper-based records that contain personal data are kept securely locked.

Personal information may only be stored on School computing devices, but staff and governors may access cloud-based services from their personal devices or via the secure VPN if off-site and are expected to follow the same security procedures as for Schoolowned equipment (see our Acceptable Use of IT Policy).

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected in transit to its destination.

Data Sharing

During the course of daily activities the School will frequently engage with third party organisations and may need to share personal data with them. A list of the third parties, with whom the School regularly shares data is available within Appendix 1.

The individuals concerned will be informed when the School shares personal data with third parties not on this list. The School will seek to ensure any third party upholds the principles of Data Protection as laid out in this document.

Personal data may be shared with a third party where:

- There is an issue with a pupil or parent/guardian that puts the safety of a pupil or our staff at risk
- We need to liaise with other agencies
 - to enable the relevant authorities to monitor the School's performance i.e. Independent Schools Inspectorate;
 - to compile statistical information (normally used on an anonymous basis);
 - to safeguard pupils' welfare and provide appropriate pastoral (and where relevant, medical) care for pupils;
 - where specifically requested by pupils and/or their parents or guardians;
 - to enable pupils to take part in national and other assessments and to monitor pupils' progress and educational needs;
 - where necessary in connection with learning and extra-curricular activities undertaken by pupils e.g. educational visits, peripatetic teachers, residential trip providers, extra-curricular providers;
 - to obtain appropriate professional advice;
 - where a reference or other information about a pupil or ex-pupil is requested by another educational establishment or employer to whom they have applied
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT support, catering
- The use by the School of online academic and educational services
- The use by the School of cloud IT services such as email and file storage for staff and pupils

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. We will only transfer personal data to a country or territory outside the EEA if we are satisfied the third party(s) involved will only process the data in accordance with data protection law.

Data Access and Subject Access Requests

Individuals have the right to request rectification of any data that is inaccurate or incomplete. In addition, individuals have the right to have their personal data erased and to prevent further processing if:

- It is no longer required for the purposes for which it was collected
- Consent is withdrawn
- There is an opposition to the processing and no superseding legitimate interest
- The personal data is being unlawfully processed
- The personal data must be removed in order to comply with a legal obligation

Individuals may request a restriction of further processing of personal data and/or object to processing on specific grounds. Individuals should submit any request to exercise these rights to the Director of Finance and Operations. If staff receive such a request, it will be forwarded to the Director of Finance and Operations.

Individuals over the age of 12 have a right of access to information held by the School about them, including:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- With whom the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject Access Requests made by parent/carers for information relating to a pupil for which they have legal responsibility may require consent from the pupil if aged 12 or over.

Decisions relating to pupil consent will be made on a case-by-case basis.

Individuals wishing to access their personal data should put their requests in writing to the Director of Finance and Operations. If a member of staff receives a Subject Access Request, it will be passed on to the Director of Finance and Operations.

The School will take reasonable steps to confirm the identity of the individual making the request and respond to any such written requests without delay and in any event, within 30 days of receipt of the request. The School may request an extension for provision of information to 90 days (3 months) of receipt of the request if the request is deemed complex. The School will

provide such information without charge. If the request is deemed unfounded or excessive, the School may deny the request as per ICO guidance.

The School will treat as confidential any reference given by the School for the purpose of the education, training or employment, or prospective education, training or employment of any pupil or member of staff. The School acknowledges that an individual may have the right to access a reference relating to them received by the School. However, such a reference will only be disclosed if such disclosure will not identify the source of the reference; or, where notwithstanding this, the referee has given consent; or if disclosure is reasonable in all the circumstances.

The School may receive requests from third parties to disclose personal data that it holds about pupils, their parents or guardians. The School will not generally disclose information unless the individual has given consent or one of the specific exemptions under GDPR applies. However, the School may wish to disclose such data as is necessary to third parties for the following purposes:

- To give a confidential reference relating to a pupil to any educational institution which it is proposed that the pupil may attend
- To give a confidential reference relating to a member of staff to any prospective employer or educational institution which that individual has responded to for employment
- To give confidential financial and salary information relating to a member of staff to any bank or building society which that individual has approached for a mortgage or loan
- To give information relating to outstanding fees or payment history to any educational institution, which it is proposed that the pupil may attend
- To publish the results of public examinations or other achievements of pupils of the School, but which does not give the name of the pupil concerned
- To disclose details of a pupil's medical condition, where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips

Where the School receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

Data Erasure and Disposal

Personal data that is no longer needed will be disposed of securely in accordance to the wishes of the data subject and the Information and Records Retention Policy.

Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

We may use a third party to safely dispose of records on the School's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Data Breaches

The School will make all reasonable endeavours to minimise the risk of personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out below. When appropriate, we will report the data breach to the ICO within 72 hours.

Based on ICO recommendation, upon finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Director of Finance and Operations. The Director of Finance and Operations will investigate the report and determine whether a breach has occurred.

In the event of a breach, the Director of Finance and Operations will alert the Headmaster and Governing Body. The Director of Finance and Operations will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. The Director of Finance and Operations will determine whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. If it is likely that there will be a risk to the rights and freedoms of an individual, the Director of Finance and Operations must notify the ICO. The Director of Finance and Operations will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. In order to make this decision, the Director of Finance and Operations will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s)

Documented decisions are stored on the Data Controller Log. As required, reports to the

ICO of a data breach will include: A description of the nature of the breach, the categories and approximate number of individuals concerned, the categories and approximate number of personal data records concerned, the name and contact details of the Director of Finance and Operations, a description of the likely consequences of the personal data breach and any measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the Director of Finance and Operations will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Director of Finance and Operations expects to have further information. The Director of Finance and Operations will submit the remaining information as soon as possible.

We will take all the necessary and practicable actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Queries and Complaints

Any comments or queries on this policy should be directed to the Director of Finance and Operations using the following email address: dfo@beaconschool.co.uk

If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with GDPR, they should utilise the School Complaints Procedure and should also notify the Director of Finance and Operations.

Appendix 1: Third parties with whom the School may share data for routine operational and educational processing:

ISC
 ISI
 IAPS
 Department for Education
 LAMDA
 Buckinghamshire County Council
 Destination Schools (after transfer)
 Accelerated Reader™
 Activelearn (Maths, Science, English)
 Adobe Creative Suite
 Alfie (Science)
 Aurasma
 BlueSky
 ClarionCall
 DADWAVERS: A Literacy Shed App
 Document Library
 Doodle
 Dropbox
 Education City / Puffin Academy
 Educreations Interactive Whiteboard
 Enchant
 Evolve
 Flickr
 GIMP
 Google+
 Hodder Dynamic Learning
 IDL Cloud iMovie iTooch
 Music Kerboodle (RS) -
 Linguascope Intermediate
 MadPad HD - Remix Your Life
 Microsoft Office 365
 Microsoft Office
 Minecraft
 Music School Manager
 My School Portal Nearpod nxCricket-
 hd - Cricket Score Book Participant
 (external clubs bookings)
 PASS / 3Sys
 Photo Editor
 Plickers
 PTO - Parents Evening bookings
 Seesaw: The Learning Journal

Showbie - Collect, review & annotate Socrative
 Teacher
 SurveyMonkey
 Testwise (VR, NVR, PTE, PTM)
 ThingLink
 Ticketsource
 Twitter
 TIARC CMS
 Wetransfer
 Yacapaca (web)
 YouTube

This list is subject to amendment and a full up to date audit list is available by emailing dfo@beaconschool.co.uk