Data Protection, Record Keeping and Retention of Records Policy

for the whole School including EYFS

Policy revised by	Amanda Barker/ Anne-Marie Ridler
SLT Review Period	3 years
Last SLT Review	September 2021
Next SLT Review Due	September 2024
Governor Review Period	3 years
Governing Committee	GP
Last Governor Review	November 2021
Next Governor Review Due	November 2024

DATA PROTECTION

1. Background

This policy is designed to ensure that the *Beechwood Park School* (hereafter 'the *School'*) complies with UK data protection law, which consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018).

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information and it is an important legal compliance issue for the *School*. During the course of the *School's* activities, it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties (in a manner more fully detailed in the *BPS Privacy Notices)*. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action.

This policy sets out the *School's* expectations and procedures with respect to processing any personal data we collect from data subjects (e.g. including parents, pupils, employees).

Key data protection terms used in this data protection policy are:

- **Data Controller** – an organisation that determines the purpose and means of the processing of personal data. For example, the *School* is the controller of pupils' personal information. As a data controller, we are responsible for safeguarding the use of personal data.

- **Data Processor** – an organisation that processes personal data on behalf of a *Data Controller*, for example a payroll provider or other supplier of services, with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

- **Personal Data Breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- **Personal Information** (or **Personal Data**): any information relating to a living individual (a data subject), including name, identification number, location, or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data

protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.

- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

- **Special Categories of Personal Data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

2. Data Protection Lead

The *School* has appointed the Bursar as the *Data Protection Lead/Chief Privacy Officer* who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the *Data Protection Lead*.

3. The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specific and explicit purposes and only for the purposes it was collected for;
- Relevant and limited to what is necessary for the purposes it is processed;
- Accurate and kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed; and
- Processed in a manner that ensures appropriate security of the personal data.

The GDPR's 'accountability' principle also requires that the *School* not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data; and

- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our *Privacy Notice(s)* were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

4. Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the *Data Controller*. It can be challenged by data subjects and also means the *Data Controller* is taking on extra responsibility for considering and protecting people's rights and interests. The *School's* legitimate interests are set out in the *BPS Privacy Policy*, as GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents; or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

5. Responsibilities of staff

Record-keeping

It is important that personal data held by the *School* is accurate, fair, and adequate. You are required to inform the *School* if you believe that your personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record the personal data of others – in particular colleagues, pupils, and their parents – is accurate, professional, and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on *School* business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the *School's* other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly, and securely and in accordance with all relevant *School* policies and procedures.

There are data protection implications across several areas of the *School's* wider responsibilities such as safeguarding and IT security.

Responsible processing also extends to the creation and generation of new personal data/records, as above, which should always be done fairly, lawfully, responsibly, and securely.

Avoiding, mitigating and reporting data breaches

One of the key new obligations contained in the GDPR is on reporting personal data breaches. *Data Controllers* must report certain types of personal data breach (those which risk an impact to individuals) to the Information Commissioner's Office (ICO) within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the *School* must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If you become aware of a personal data breach you must notify the Bursar. If you are in any doubt as to whether you 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 it to make a decision.

As stated above, the *School* may 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, and could be a serious disciplinary matter whether under this policy or the staff member's contract.

6. Rights of Individuals

In addition to the *School's* responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the *School*). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Bursar as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and

- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);

- object to direct marketing; and

- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Bursar as soon as possible.

7. Data Security: online and digital

The *School* must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Consequently, we require all *School* staff to remain conscious of the data protection principles (see section 3 above), to attend any training we require them to, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management or leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the *School* to the Bursar, and to identity the need for (and implement) regular staff training.

Records – whether electronic or hard copy – are stored securely, including if possible with encryption, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable;

Questions of back-up or migration are likewise approached in line with general *School* policy (such as professional storage solutions or IT systems) and not individual *ad hoc* action.

Arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage) – are supported by robust contractual arrangements providing for security and access.

No member of staff is permitted to remove personal data from *School* premises, whether in paper or electronic form and wherever stored, without authority. For routine activities such as sports fixtures or trips this may be granted by Heads of Departments. In all other instances prior consent from a member of the SLT is required. Data taken off site must be encrypted where possible. Paper copies must be physically secured at all times whilst off site and must be destroyed securely on return to *School*. Use of personal email accounts or unencrypted personal devices for official *School* business is not permitted.

Important records, and large or sensitive personal databases, are not to be taken home or – in respect of digital data – carried or kept on any portable devices (including CDs, memory sticks, mobiles, or other handheld electronic devices).

The use of personal devices to record images of *School* activities involving pupils, staff or parents is strictly forbidden.

RECORD KEEPING

1. Current Pupils

A file is kept on each pupil in the *School Office*. The file holds the registration and acceptance form, the parent contract, and the academic record of a pupil as he or she progresses through the *School*. It will also include reports of all conversations between parents and members of staff about any academic or pastoral issues, school reports, references from previous schools and references prepared for future schools. It will record any disciplinary sanctions imposed on a pupil.

The information held on the *School's* electronic database covers: the pupil's name, address, form, house, emergency contact details, academic performance, pastoral records (including rewards and sanctions), subjects studied and daily attendance.

The *Designated Safeguarding Lead* (DSL) keeps records of those pupils giving cause for concern (C4C).

2. Pupils with Special Educational Needs or Medical Needs

The names of pupils with special educational or medical needs are recorded on the *School's* database.

Detailed information on the special educational needs of individual pupils, such as assessment reports and Learning Support Pupil Plans, are stored on the staff network drive and in pupil files, held by the *Learning Support Department*.

3. Medical Records

A confidential medical record on each pupil is kept securely in the *Surgery* and on the *School's* database. The record contains: contact details of the pupil's GP; the medical questionnaire that the parents completed when their child joined the *School*; individual health care plans and daily routines where appropriate; records of all surgery visits, treatment, and immunisations that a pupil receives; records of all accidents and injuries.

The *Surgery* staff will provide a list of the names of current pupils with medical conditions, or social information of a sensitive nature that may be of relevance to staff in their dealings with pupils; for example, in the boarding house, in class, on the sports fields, or for trips and visits.

4. Financial Records

The *Bursary* holds financial records on all pupils throughout their career at the *School*: a record of the deposit; the acceptance form; invoices for tuition fees and extras; correspondence concerning default of payment. If a pupil receives a bursary or scholarship, this will form part of the record, along with parents' applications, records of annual assessments and awards.

5. Access by Staff

All teaching and office staff can access the *School's* password-protected database, although the extent of that access is limited to that which is required for the effective performance of their duties. Teaching staff may consult the pupil records held in the *School Office*, redacted as required by the Head's Secretary/Registrar. Access to medical records is restricted to the Surgery staff, Head and Bursar. Access to financial records is restricted to the Head, Bursar and the Finance staff.

6. Past Pupils

The *School* keeps records of past pupils in accordance with the criteria at *Appendix 1*. The *School* retains records of results in public examinations, lists of *School* prizes and other significant achievements, together with information relating to former pupils' subsequent academic achievements. Records relating to alumni are stored in the *School's* archives and on the *School's* database.

RETENTION OF RECORDS

1. Principles

The *School's* policy on retention periods for various categories of data is laid out in *Appendix 1*.

Reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and – in the case of personal data – necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date).

2. Disposal

For confidential, sensitive, or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Skips and 'regular' waste disposal will not be considered secure.

Paper records should be shredded using a cross-cutting shredder; CDs/DVDs/diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed.

Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the *School* to process and dispose of the information.

3. Data Breaches

Where a security incident takes place, the *School* will quickly establish whether a *Personal Data Breach* has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

A *Personal Data Breach* can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authority; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is about more than just losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a *Controller* or *Processor*;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and

- loss of availability of personal data.

Potential breaches are to be reported to the Bursar without delay.

The *School* will report a breach if it will result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Such matters may separately require a report to the Charity Commission.

APPENDICES BELOW:

Appendix 1

RETENTION PERIODS

Type of Record/Document	Retention Period
SCHOOL-SPECIFIC RECORDS	
• Registration documents of the School	Permanent (or until closure of the School)
• Attendance Register	6 years from date of last entry, then archive
• Minutes of Governors' Meetings	Minimum – 10 years from date of meeting
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments
INDIVIDUAL PUPIL RECORDS	
• Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision)
• Examination results (external or internal)	7 years from pupil leaving school
• Pupil files including: o Pupil reports o Pupil performance records o Pupil medical records	ALL: 25 years from date of birth (subject where relevant to safeguarding considerations): any material which may be relevant to potential claims should be kept for the lifetime of the pupil
• Special educational needs records (*to be risk assessed individually*)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
SAFEGUARDING	
• Policies and procedures	Keep a permanent record of historic policies
• DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
• Incident reporting	Keep on record for as long as any living victim may bring a claim and for a minimum of 25 years (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.
• Child Protection files	If a referral has been made/social care have been involved or child has been subject of a

	multi-agency plan – indefinitely. If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).
CORPORATE RECORDS • Certificates of incorporation • Minutes, notes and resolutions of Board or management meetings • Shareholder resolutions • Register of members • Annual reports	 Permanent (or until dissolution of the company) Minimum – 10 years Minimum – 10 years Permanent (minimum 10 years for ex-members) Minimum – 6 years
ACCOUNTING RECORDS • Accounting records including tax returns • Budget and internal financial reports	 Minimum – 6 years from the end of the financial year in which the transaction took place Minimum – 3 years
CONTRACTS AND AGREEMENTS • Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*) • Deeds (or contracts under seal)	 Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS • Formal documents of title (trade mark or registered design certificates; patent or utility model certificates) • Assignments of intellectual property to or from the School • IP/IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence	 Permanent (in the case of any right which can be permanently extended, e.g. trade marks); otherwise, expiry of right plus minimum of 7 years As above in relation to contracts (7 years) or, where applicable, deeds (13 years) Minimum – 7 years from completion of contractual obligation concerned or term of agreement

agreements; consents)	
EMPLOYEE/PERSONNEL RECORDS	
• Single Central Register of Employees	Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above)
• Contracts of employment	7 years from effective date of end of contract
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file	Minimum 7 years – subject to safeguarding considerations as described above. Do not delete any information which may be relevant to historic safeguarding claims.
• Payroll, salary, maternity pay records	Minimum – 6 years
• Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme
• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
• Immigration records (Right to Work etc)	Minimum – 2 years from end of employment
• Health records	7 years from end of contract of employment
INSURANCE RECORDS	
• Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim
• Correspondence related to claims/ renewals/notification re: insurance	Minimum – 7 years (*but this will depend on what the policy covers and whether e.g. historic claims may still be made*)

ENVIRONMENTAL, HEALTH AND DATA	
• Maintenance logs	10 years from date of last entry
• Major accidents to pupils (referred to emergency services or RIDDOR report)	25 years from birth (longer if safeguarding issues)
• Accidents at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case where possible
• Staff use of hazardous substances	Minimum – 7 years from end of date of use
• Covid-19 risk assessments, consents, notices etc *(subject to further review)*.	Retain for now legal paperwork (consents, notices, risk assessments), but not individual test results.
• Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event, or activity
• Data protection records documenting processing activity, data breaches	No limit: as long as up-to-date and relevant (as long as no personal data held)