Belmont Preparatory School
Storage and Retention of Data and Documents

1 Introduction

1.1 This policy is intended to provide information about how the School will store and retain records and documents relating to the School, its staff or pupils. This will include data about individuals including: its staff, governors and volunteers; its current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents").

1.2 The General Data Protection Regulation (GDPR) from 25 May 2018 requires that the storage and retention of records and documents is relevant, purposeful and secure.

1.3 The GDPR also means that the School must ensure:

- All information held needs to be justifiable, by reference to its purpose;
- The systems of record retention must be transparent and accountable;
- That there is an understanding and explanation of the reasons for holding data, which also means keeping records that explain how decisions around personal data are made;
- It is prepared to respond more quickly to subject access requests;
- That it must be able to amend, delete or transfer data promptly upon any justified request, or otherwise prepared to explain why we will not;
- That there is an audit trail for the collection and storage of data; and that
- Sensitive data is held securely and accessed only by those with reason to view it.

2 Scope of this Policy

2.1 This policy applies alongside any other information the School may provide about the use of personal data, and in addition to the School's other relevant terms and conditions and policies, including:

a) any contract between the School and its staff or the parents of pupils, and consent forms;

b) the School's policy on Taking, Storing and Using Images of Children;

c) the School's Safeguarding Policy, Health and Safety Policy; and

d) the School's IT policies, including its Online Safety Policy, and Acceptable Use Policies and Agreements; and

e) The Privacy Notice and the Staff Privacy Notice.

2.2 The School will seek to balance the benefits of keeping detailed and complete records (for the purposes of good practice, archives or general reference) with practical considerations of storage, space and accessibility. In addition, there are

legal considerations in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to schools, including for safeguarding;
- disclosure requirements for potential future litigation;
- contractual obligations;
- the law of confidentiality and privacy; and
- the GDPR and UK domestic Data Protection Act 2018 (DPA).

These will inform not only minimum and maximum retention periods, but also what to keep and who should be able to access it.

3 Definitions

3.1 In this Policy, "record" means any document or item of data which contains evidence or information relating to the School, its staff or pupils. Some of this material, but not all, will contain personal data of individuals as defined in the GDPR. An obvious example of personal data would be the Single Central Record or a pupil file; however, a "record" of personal data could arise simply by holding an email on the School's systems.

3.2 Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers, or older records) will be original paper documents. Within the context of GDPR, the format of the record is less important than its contents and the purpose for keeping it. The School has reviewed the records and documents retained and the retention periods appropriate to those records, depending on the purpose. Legal requirements have also been taken into account, and the information is provided in the Appendix.

3.3 Digital records can be lost or misappropriated in huge quantities very quickly. Therefore, access to sensitive data (or any large quantity of data) is password-protected and digital encryption is applied. Passwords are regularly changed.
A digital document's original metadata may indicate the date of its creation, its author or the history of its changes: so it is important that this information is also preserved.

3.4 Emails (whether they are retained electronically or printed out as part of a paper file) are also "records" and may be particularly important: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record.

3.5 Paper records are most often damaged by damp or poor storage conditions; but as well as applying common sense (i.e. dry, cool, reasonable ventilation, no direct sunlight; avoid storing with metals, rubber or plastic which might deteriorate or damage the paper), security is also vital – especially if the materials contain legally or financially sensitive data, as well as data personal to individuals.

3.6 Under the DPA, paper records are only classed as personal data if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible, and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category: but a merely chronological file of correspondence may well not. However, when personal information is contained on print-outs taken from electronic files, this data has already been processed by the School and therefore falls under the DPA.

3.7 Personal data means information about individuals eg. staff, pupils, consultants, parents, contractors – or indeed other individuals, whether they are a part of the School or some other third party (for example, another school). Personal data includes: contact and communications information, biographical, educational or social information, financial and work-related information. It includes everything from which a data subject can be identified. It ranges from simple contact details via personnel or pupil files to safeguarding information, and encompasses opinions, file notes or minutes, a record of anyone's intentions towards that person, and communications (such as emails) with or about them.

3.8 Sensitive personal data includes information relating to an individual in respect of their health, race, religion, sexual life, trade union membership, politics or any criminal proceedings, offences or allegations.

4 Storage, Retention and Destruction of Records

4.1 The table at Appendix 1 provides guidance on the retention of records held by the School. It is provided to assist staff in identifying the key types of document related to this Policy and action that should be taken, except where there is a specific statutory obligation to destroy records. If in any doubt about the storage, retention or destruction of records, staff should seek advice from the Head or Bursar.

4.2 There are various categories of records:

- Accounting
- Contracts and Agreements
- Corporate
- Data
- Employee/Personnel records
- Environmental and Health
- Individual pupil records
- Insurance records
- Property records
- Safeguarding
- School-specific records

4.3 On a day-to-day basis, the School mainly uses electronic methods of data storage and retention. As part of the induction process, all new staff, governors and visitors who have been provided with access to the School's network are issued with the IT Acceptable Use Agreement/Code of Conduct which they will be expected to sign, and a copy of this will be kept on file.

4.4 ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are part of daily working life in school and the Agreement is designed to ensure that all staff, governors and visitors are aware of their professional responsibilities when using any form of ICT, particularly with regard to security and access to data.

4.5 The School's Online Safety Policy provides guidance on the use of passwords to protect access to electronic records. Certain types of data have restricted access, and this relates to digital and paper records. Staff may use encrypted USB devices provided by the School to assist with remote working.

4.6 Records are stored on school servers which staff may access via secure links, depending on the software, and no data leaves the system for the outside world. Data is held on an encrypted volume which only the company managing the software knows, and encrypted URLs (Uniform Resource Locators) are used when accessing files on the School's VLE.

4.7 Mobile devices, e.g. iPads, used by the School are also managed via the use of passwords, and this information will be integrated into a new iboss cloud platform within in a UK storage facility. The only data stored will be the username and password (a password for the Mobile Device Management System only). The School uses Microsoft Office for email communication and it has been confirmed that the Office 365 data, including emails, is also stored in the UK.

4.8 The School's computer systems are backed-up on a daily basis on a separate stand-alone server. The system is managed and checked by the IT Manager.

4.9 Reviews of data are conducted on a regular basis in line with the guidance in the Appendix 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.

4.10 Destruction or permanent erasure of records, when undertaken by a third party, is carried out securely, with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them. Where third party disposal experts are used, they are under adequate contractual obligations to the School to process and dispose of the information. 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 are not secure and therefore should not be used for disposal.

4.11 For on-site disposal, paper records are shredded using a cross-cutting shredder. CDs/DVDs/diskettes are cut into pieces, hard-copy images, AV recordings and hard disks will be dismantled and destroyed.

Authors: Helen Skrine, Headmistress & Claire Candlish, Bursar

Date: May 2018

Approved by: Legal & Compliance Committee

Date: May 2018

Review Due: Lent 2019

Appendix 1

Type of Record/Document	**Suggested [1] Retention Period**
SCHOOL-SPECIFIC RECORDS • Registration documents of School • Attendance Register • Minutes of Governors' meetings • Annual curriculum	Permanent (or until closure of the school) 3 years after end of school year in question, then archive. 6 years from date of meeting, then archive. From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS • Admissions: application forms, assessments, records of decisions • Examination results (external or internal) • Pupil file including: o Pupil reports o Pupil performance records o Pupil medical records • Special educational needs records	***NB – this will generally be personal data*** All records retained until the child reaches age 18. The following then applies to all remaining categories of individual pupil records unless there is a Safeguarding consideration or a perceived risk of a potential claim against the School. In these circumstances records are kept for the lifetime of the individual. Paper Records Retained until end of year following 100th birthday of pupil, Electronic Records Retained until end of 5th year following leaving the School. For alumni, date of birth/death/primary contact detail will be retained indefinitely. All records (paper and electronic) will be kept until the pupil attains the age of 25 years, or kept longer if warranted by risk assessment).

SAFEGUARDING	
• Policies and procedures	A permanent record of historic policies will be kept on the School VLE
• DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted. A record of the checks being made is kept.
• Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (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. [2]
• Child Protection files	If a referral has been made or social care have been involved, or child has been subject of a multi-agency plan, records are kept indefinitely. If low level concerns, with no multi-agency action, records will be kept 100 years from date of birth. Where Safeguarding files are transferred if/when the child transfers to another school, an indefinite record will be kept of the transfer.

CORPORATE RECORDS	All records will be kept permanently
• Certificates of Incorporation	
• Minutes, Notes and Resolutions of Boards or Management Meetings	
• Shareholder resolutions	
• Register of Members/Shareholders	
• Annual reports	

ACCOUNTING RECORDS [3]	
• Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*)	Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place
• Tax returns	Minimum – 6 years
• VAT returns	Minimum – 6 years
• Budget and internal financial reports	Minimum – 6 years
CONTRACTS AND AGREEMENTS	
• Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
• Deeds (or contracts under seal)	Indefinitely
INTELLECTUAL PROPERTY RECORDS	
• Assignments of intellectual property to or from the School	Permanent

EMPLOYEE / PERSONNEL RECORDS	***NB this will contain personal data***
• Single Central Record 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	100 years from date of birth of employee or upon their death
• Employee appraisals or reviews	Duration of employment plus 7 years
• Staff personnel file	As above, but 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	Minimum – 6 years
• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 5 years
• Immigration records	100 years from date of birth
• Health records relating to employees	100 years from date of birth
INSURANCE RECORDS	
• Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) or 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
ENVIRONMENTAL, HEALTH & DATA	
• Maintenance logs	6 years from date of last entry
• Accidents to children [4]	Indefinitely for major incidents and minor incidents on a case-by-case basis.
• Accident at work records (staff) [4]	
• Staff use of hazardous substances [4]	Minimum – 6 years from end of date of use
• Risk assessments (carried out in respect of above) [4]	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)

FOOTNOTES:

1. General basis of suggestion:

   Some of these periods will be mandatory legal requirements (eg under the Companies Act 2006 or the Charities Act 2011), but in the majority of cases these decisions are up to the institution concerned. The suggestions will therefore be based on practical considerations for retention such as limitation periods for legal claims, and guidance from Courts, weighed against whether there is a reasonable argument in respect of data protection.

2. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches. It also found that it would be disproportionate for most organisations to conduct regular reviews, but at the time of writing the ICO (Information Commissioner's Office) still expects to see a responsible assessment policy (eg every 6 years) in place.

3. Retention period for tax purposes should always be made by reference to specific legal or accountancy advice.

4. Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this: so keep a note of all procedures as they were at the time, and keep a record that they were followed. Also keep the relevant insurance documents.