****

**Data Retention & Storage Guidance**

**This document details the types of records/data held by the School, and how long the data should be retained. It is important that this document is read in conjunction with the School’s latest Privacy and Data Protection Policy.**

**The School ensures that data is stored in line with:**

* **Statutory duties and government guidance relating to schools, including safeguarding;**
* **Disclosure requirements for potential future litigation;**
* **Contractual obligations;**
* **The law of confidentiality and privacy;**
* **The General Data Protection Regulations 2018**
* **Current school insurance policy**

**All staff will receive some basic training in data management and will be required to complete the online GDPR course provided by the School’s online training provider. Senior management will receive additional training relating to their specific role.**

**Meaning of ‘Record’**

**In these guidelines, 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 Data Protection Regulations.**

**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.**

**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. The format of the record is less important than its contents and the purpose for keeping it.**

**Digital Records**

**Digital records can be lost or misappropriated in huge quantities very quickly, therefore, Notre Dame Prep School ensures that all key forms of electronic storage are password protected i.e. SIMS database, ~~SAGE~~ Payroll & Accounts etc. The school operates a firewall on its server called Securely that provides protection against external attack.**

**Digital records must not be kept on portable devices (whether CDs or data sticks, or mobiles and handheld electronic tablets) unless absolutely necessary, in which case, it would be subject to a risk assessment and in line with our IT Acceptable Use Policy and Working from Home Policy.**

**All teaching staff have a formal school email address. All school email addresses can be monitored via the school systems and protected are protected by the school firewall. Personal emails are not used for school business. Staff personal emails are not known to parents.**

**School governors have NDPS emails as well such that sensitive material remains on the school server.**

**Paper Records**

**The school must ensure the appropriate storage of paper records. Paper records will be stored securely in a damp free environment. Paper records pertaining to admissions and personnel will be filed and organised in locked filing cabinets located in the main school office along with other sensitive information such as SEN files. Safeguarding files are kept locked away in the DSL’s office.**

**Day to day records such as the class mark books and some information relating to SEN are kept in the classroom but always in the teacher’s desk and never on general display. The majority of the paper records will be transferred onto the school management information system SIMS at the appropriate points throughout the year.**

**Archiving and the destruction or erasure of Records**

**Paper records are destroyed by shredding in-house; CDs / DVDs/ diskettes should be cut into pieces. Hard-copy images, AV recording and hard disks should be dismantled and destroyed.**

**The school ensures that all destruction or permanent erasure of records, if undertaken by a third party i.e. our IT support, Net Central, is carried out securely – with no risk of the re-use or disclosure, or reconstruction of any records or information contained in them.**

**The school has guidelines for the retention periods of data – see Annex A, however, it is important to note that some data may be kept for longer if legally required to or in cases where there is potential for litigation. This reason for keeping data longer than normally required needs to be considered by the SMT very carefully. Keeping lots of data for long periods can lead to increases in the administrative and storage burden on the school and, in addition, this also increases the amount of material in respect of which the school is accountable to data subjects (e.g. information requests, “right to be forgotten” requests), which could potentially result in serious security breach consequences.**

**This guidance must be read in conjunction with the schools Privacy & Data Protection Policy which outlines the purpose, relevance and accuracy of the information held.**

***Reviewed September 2025 by S Smith***

***Approved September 2025 by L Campbell***

***To be reviewed no later than September 2026***

***Annex A***

**GUIDELINES FOR DATA RETENTION PERIODS**

|  |  |
| --- | --- |
| **Type of Record/Document** | **Retention Period** |
| SCHOOL-SPECIFIC RECORDS * Registration documents of School
* Attendance Register
* Minutes of Governors' meetings
* Annual curriculum
 | Permanent (or until closure of the school) 6 years from last date of entry, then archive.  6 years from date of meeting  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 and correspondence.
* Examination results (external or internal)
* Pupil file including:

o Pupil reports o Pupil performance records o Pupil medical records * Special educational needs records (*to be risk assessed individually*)
 | 9 years from pupil leaving the school. In the case of a non-starter – 2 years from date of the withdrawal of the application.  9 years from pupil leaving school  ALL: 7 years from date of leaving (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil).  9 years from date of leaving (allowing for special extensions to statutory limitation period)  |
| SAFEGUARDING * Policies and procedures
* DBS disclosure certificates (if held)

  * Accident / Incident reporting
* Child Protection files

 | Keep a permanent record of historic policies 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*.* 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. 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 actions or involvement– apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely). |
| ACCOUNTING RECORDS * 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*)

[NB specific ambit to be advised by an accountancy expert] Budget and internal financial reports |  Minimum – 6 years for UK charities (and public companies) 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 agreements; consents)
 |  Permanent (in the case of any right which can be permanently extended, eg 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 for term of agreement |
| EMPLOYEE/PERSONNEL RECORDS* Single Central Register
* Contracts of employment
* Employee appraisals or reviews
* Staff personnel file
* Payroll, salary, maternity pay records
* Pension or other benefit schedule records
* Job application and interview/rejection records (unsuccessful applicants)
* Immigration records
* Health records relating to employees
 | Keep a permanent record of all mandatory checks that have been undertaken. The DBS will be kept on file for the duration of the employment and destroyed upon leaving10 years from effective date of end of contractDuration of employment plus minimum of 10 yearsAs above, but do not delete any information which may be relevant to historic safeguarding claimsMinimum – 10 yearsMinimum 7 yearsPossibly permanent, depending on nature of schemeMinimum 3 months but no more than 1 year4 years10 years from end of contract of employment |
| INSURANCE RECORDS* Insurance policies (will vary – private, public, professional indemnity
* Correspondence related to claims/renewals/notification re: insurance
 | 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 claimMinimum – 7 years |
| ENVIRONMENTAL, HEALTH & DATA* Maintenance logs
* Accidents to children (serious)
* Accidents to children (minor)
* Accident at work records (staff)
* Staff use of hazardous substances
* Risk assessments (carried out in respect of above)
* Data protection records documenting processing activity, data breaches
 | 10 years from date of last entry25 years from birth (longer for safeguarding)Minimum – 2 years from date of accidentMinimum – 4 years from date of accident, but review case-by-case where possibleMinimum – 7 years from end of date of use 7 years from completion of relevant project incident, event or activityNo limit: as long as up-to-date and relevant (as long as no personal data held) |