OLD BUCKENHAM HALL

A leading co-educational preparatory school for children aged 2-13 years

GDPR Policy

OBHP43

Policy owner: Director of Finance and Operations
Date of issue: August 2019
Date last reviewed: August 2023
Next review due: August 2024

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics

	• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Assistant Bursar
The Assistant Bursar (HR) is responsible for monitoring our compliance with data protection law also investigating alleged breaches in the security of data and for annually reviewing this policy.

They will report to the Director of Finance and Operations any data processing issues and, where relevant, provide advice and recommendations.

The Assistant Bursar is also the first point of contact for individuals whose data the school processes, and for the ICO.

alex.rashbrook@obh.co.uk or 01449 740227

5.3 The Director of Finance & Operations (DFO)
The DFO acts as the representative of the data controller on a day-to-day basis.

5.4 All staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Assistant Bursar in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles
The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed

- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency
We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law – this will be in the form of a privacy notice.

The current privacy notices for each relevant category of data subject can be found on the school website and relate to staff, governors, parents and students.

7.2 Limitation, minimisation and accuracy
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

This includes:

- 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
- Who 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 must be submitted in writing to the Assistant Bursar. A template form for this purpose can be found in Appendix 2.

If staff receive a subject access request, they must immediately forward it to the Assistant Bursar.

9.2 Children and subject access requests
Personal data about a child belongs to that child, and not the child's parents or carers.

For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our **Prep School** may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests
When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee, which takes into account administrative costs. A request will be deemed unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Assistant Bursar. If staff receive such a request, they must immediately forward it to the Assistant Bursar.

10. Parental requests to see the educational record

The parents of children under 13 may request the educational records of their children. The school will provide a copy of the elements of the educational records when such requests are received.

11. Biometric recognition systems

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will achieve written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can be registered manually if they wish.

Parents/carers and pupils can object to participation in any proposed school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Should our school staff members or other adults use a new biometric system, we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

Please see our school's Security Policy

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

14. Data protection by design and default

We will put measures 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 set out in relevant data protection law
- 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 (the Assistant Bursar will advise on this process)
- Integrating data protection 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 a record of training
- Annually conducting a review and audit to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and Assistant Bursar and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

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 and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals. Students have limited access to school systems.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see Pupil and Staff Code of Conduct, ICT Code of Conduct).
- 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.

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. 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.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also 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.

17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors are made aware of the GDPR policy and Privacy Notices as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

The Assistant Bursar and Director of Finance and Operations are responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice.

Otherwise, or from then on, this policy will be reviewed on an annual basis and shared with the full governing board.

20. Links with other policies

This data protection policy is linked to our:

- Data Retention Schedule
- ICT Code of Conduct for staff and students
- Governor Privacy policy
- Student Privacy Policy
- Employee Privacy Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Assistant Bursar
- The Assistant Bursar will investigate the report and determine whether a breach has occurred. To decide, the Assistant Bursar will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Assistant Bursar will alert the DFO & Head who will inform the Chair of Governors
- The Assistant Bursar will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The Assistant Bursar will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Assistant Bursar will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Assistant Bursar 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 through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it is likely that there will be a risk to people's rights and freedoms, the Assistant Bursar must notify the ICO.
- The Assistant Bursar will document the decision (either way), in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored in the school's data breach log.

- Where the ICO must be notified, the Assistant Bursar will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Assistant Bursar will set out:
    - A description of the nature of the personal data breach including, where possible:
        - 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 Assistant Bursar
    - A description of the likely consequences of the personal data breach
    - A description of the 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 Assistant Bursar 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 Assistant Bursar expects to have further information. The Assistant Bursar will submit the remaining information as soon as possible
- The Assistant Bursar will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Assistant Bursar will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the Assistant Bursar
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Assistant Bursar will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Assistant Bursar will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's data breach log.
- The Assistant Bursar, DFO and Head will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches
We will take a range of appropriate 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.

For example, sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the Assistant Bursar as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Assistant Bursar will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the Assistant Bursar will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The Assistant Bursar will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Assistant Bursar will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Old Buckenham Hall Data Breach Incident Form

Under the General Data Protection Regulation 2016 and the Data Protection Bill 2017, organisations, which process personal data, must take appropriate measures against unauthorised or unlawful processing and against loss, destruction of or damage to personal data. A data security breach can happen for a number of reasons:

1. Loss or theft of data or equipment on which data is stored
2. Inappropriate access controls allowing unauthorised use
3. Equipment failure
4. Human error
5. Unforeseen circumstances such as a fire or flood
6. Hacking attack
7. 'Blagging' offences where information is obtained by deceiving the organisation who holds it

As soon as you are aware of a data breach you must notify the Assistant Bursar within 24 hours by completing this form and return to: alex.rashbrook@obh.co.uk**.**

1.	Name of the person who identified the breach	
2.	Job title and contact details	
3.	School Name	
4.	Date incident occurred	
5.	Is this a breach of data by a supplier or partner organisation? (If the breach has been notified to you by a supplier or a partner organisation who you share your data with, name of the supplier/partner, date notified, contact should be completed)	The breach originated in school: **Yes/No** We have been notified of the breach by a supplier / Partner Organisation. **Name:** **Name Contact:** **Date Notified:** **[Insert Link to the saved notification]**
5.	Who has been notified of the breach to date? (e.g. Head, Executive Officer, ICO, Parents, Teachers, Governors etc.)	
6.	Type of data involved and how sensitive is it? (Some data is sensitive because of its very personal nature e.g. social services and health records. Other data types are sensitive because of what might happen if it is misused e.g. bank account details.)	

7.	If the data has been lost or stolen, were there any protections in place such as encryption?	
8.	What Type of Data Breach is it? A **Confidentiality Breach** has occurred if the data was unauthorised of accidentally disclosed. An **Availability Breach** has occurred if the data was unauthorised or accidentally lost. An **Integrity Breach** has occurred if the data was unauthorised or accidentally altered.	Delete as applicable: Confidentiality Breach: Yes/No Accidental/Unauthorised Availability Breach: Yes/No Accidental/Unauthorised Integrity Breach: Yes/No Accidental/Unauthorised
9.	What could the data tell a third party (individual or organisation) about the school/pupil/teacher? For example, sensitive data could disclose an individual's medical condition, details of their finances.	
10.	How many individuals' personal data are affected by the breach?	Approx. Number individuals impacted: Who are they (staff, children etc.) Approx. Number of data records impacted:
12.	What harm could be caused by the breach, consider whether there is: Any risks to physical safety as a result of the breach? Any risks of the data being used to discriminate against and individual? Any risks to the reputation of any individual being impacted by the breach? Any risks of financial loss through identity theft?	**The ICO will need to be notified within 72 hours of all data breaches where a risk to individual's rights and freedom exists.** If you have answered yes to any of the questions on the left-hand side, it is likely that you will need to notify the breach to the ICO.
13.	Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?	

Signature: _____

Print Name: _____

Job Title: _____

Date: _____

To be completed by the Assistant Bursar
Date received and logged: Date ICO notified: Actions taken to recover in full or partially the data: Does this represent a 'High Risk' to the rights and freedoms of those impacted individuals? If yes details of the communication plan: Future mitigating actions identified: Date added to the General Data Protection Compliance Action Plan:

Signature: _____

Print Name: _____

Job Title: _____

Date: _____

Review Date: _____

Appendix 2: Subject access request form

Name:
Telephone Number:
Email:
Address:
Employee Payroll Number *(If relevant)***:**
By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you by the school that you are eligible to receive.
Required information (and any relevant dates): *Example: Emails between "A" and "B" from 1 May 2017 to 6 September 2017.*
By signing below, you indicate that you are the individual named above. The school cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, cost and expenses if you are not. Please return this form via email to the Assistant Bursar on alex.rashbrook@obh.co.uk Please allow 1 calendar month for a reply.
Data Subject's Signature:
Date:

Appendix 3

OLD BUCKENHAM HALL DATA RETENTION SCHEDULE

Type of Record/Document	Suggested Retention Period
SCHOOL-SPECIFIC RECORDS	
• Registration documents of School	Permanent (or until closure of the school)
• Attendance Register	6 years from last date of entry, then archive
• Minutes of Governors' meetings	6 years from date of meeting
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: eg marks/timetables/assignments)
INDIVIDUAL PUPIL RECORDS	***NB - this will generally be personal data***
• 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 file including: o Pupil reports o Pupil performance records o Pupil medical records	ALL: 25 years from date of birth* * *unless there is good reason to consider this may be applicable evidence in a medical negligence or abuse claim:* see 'Safeguarding' below.
• Special educational needs records *(to be risk assessed individually)*	Date of birth plus up to 35years (allowing for special extensions to statutory limitation period)
SAFEGUARDING	
• Policies and procedures	Keep a permanent record of historic policies
• DBS disclosure certificates (potentially sensitive personal data & must be secure)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted - but keep a record of the fact that checks were undertaken, if not the information itself).
• Incident reporting	Keep on record for 35 years, ideally reviewed regularly (eg every 6 years)
CORPORATE RECORDS (where applicable)	***Eg. where schools have trading arms***
• Certificates of Incorporation	Permanent (or until dissolution of the company)
• Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum - 10 years

• Shareholder resolutions	Minimum - 10 years
• Register of Members/Shareholders	Permanent (minimum 10 years for ex members/ shareholders)
• Annual reports	Minimum - 6 years
ACCOUNTING RECORDS	
• Accounting records *(normally taken taken to mean records which enable a company's accurate financial position to be ascertained* & *which give a true and/air 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 Internationally: can be up to 20 years depending on local legal/accountancy requirements
• 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)	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)	Permanent (in the case of any right which can be permanently extended, eg. trade marks); otherwise expire of right plus minimum of 7 years.
Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
IP/ IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; co-existence agreements; consents)	Minimum - 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE/ PERSONNEL RECORDS	***NB this will almost certainly be personal data***
• Contracts of employment	Minimum - 7 years from effective date of end of contract

• Employee appraisals or reviews and staff personnel file	Duration of employment plus minimum of 7 years
• 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 years (but see note of DBS disclosure certificates above)
• Immigration records	Minimum - 4 years
• Health records relating to employees	Minimum of 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
ENVIRONMENTAL & HEALTH RECORDS	
• Maintenance logs	10 years from date of last entry
• Accidents to children	25 years from birth (unless safeguarding incident)
• Accident 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
• Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity