Newland House School

Data Protection Policy

Updated	**September 2024**
Updated by	**Bursar**
Authorised by	**Chris Skelton, Head** **Governing body**

This Policy applies to all sections of the school, including the Early Years Foundation Stage

Contents

1. Introduction

1.1 Data protection is an important legal compliance issue for Newland House 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 School's Privacy Policy). 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.

1.2 UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the "UK GDPR") and the Data Protection Act 2018 ("DPA 2018"). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

1.3 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. The Information Commissioner's Office ("ICO") is responsible for enforcing data protection law in the UK and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

1.4 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 intentional and serious breach of this policy may result in disciplinary action.

1.5 This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (for example, 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.
- 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.

1.6 The school will follow procedures that aim to ensure that all governors, teachers, administrative staff, facilities staff, peripatetic music staff, members of the Parents Association (PA) and external temporary consultants who have access to any personal data held by or on behalf of the school, are fully aware of and abide by their duties and responsibilities under the Act.

2. Data Protection Controller

2.1 The School has appointed the Bursar as the Data Protection Controller 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 Controller.

3. The Principles

3.1 UK 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:

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

3.2 UK 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

4.1 Under UK 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 generally considered preferable to rely on another lawful ground where possible.

4.2 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 Controller. It can be challenged by data subjects and also means the Controller is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Policy, as UK GDPR requires.

4.3 Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity.
- contractual necessity, for example, to perform a contract with staff or parents.
- 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 all staff

Record-keeping

5.1 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. Details of how staff's data is managed is set out in the Staff Privacy Notice in Appendix 1. Similarly, it is vital that the way you are recording the personal data of others – in particular colleagues, pupils and their parents – is accurate, professional and appropriate.

5.2 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

5.3 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. In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Digital Strategy Policy
- Safeguarding and child protection policy
- Digital Image policy
- Staff Handbook

5.4 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

5.5 One of the key new obligations contained in UK 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 ICO within 72 hours.

5.6 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 will 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 staff are in any doubt as to whether or not 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 them to make a decision.

5.7 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.

Care and data security

5.8 More generally, 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 effects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

5.9 We expect all those with management / 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.

6. Rights of Individuals

6.1 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.

6.2 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.
- 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 and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

6.3 Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. 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

7.1 The School will 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. As such, no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and

wherever stored, without prior consent of the Head or Bursar. If you have been given permission to take data offsite it will need to be encrypted. Use of personal email accounts or unencrypted personal devices for official School business is not permitted. For further information please see Digital Strategy policy.

8. Rights of Access to Information

8.1 Staff have the right of access to information held by the School, subject to the provisions of the Data Protection Act 1998. Any member of staff wishing to access their personal data should put their request in writing to the HR and Compliance Manager. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 30 days for access to records and 21 days to provide a reply to an access to information request. The information will be imparted to the worker as soon as is reasonably possible after it has come to the School's attention.

9. Retention of data

a. The table at Appendix 2 has three main functions:
   - it helps us to identify the key types of document concerned.
   - it focuses attention on any particular issues associated with those types of document.
   - it acts as an outline guide only.

b. Except where there is a specific statutory obligation to destroy records, it is misleading to present (or apply) any guidance as if it constitutes prescriptive time 'limits'. Figures given are not intended as a substitute to exercising thought and judgment, or take specific advice, depending on the circumstances.

c. It is necessary to exercise thought and judgment – albeit that practical considerations mean that case-by-case 'pruning' of records may be impossible. It is accepted that sometimes a more systemic or broad-brush approach is necessary, which is where the table comes in.

10. Exemptions

a. Certain data is exempted from the provisions of the Data Protection Act which includes the following:
   - The prevention or detection of crime.
   - The assessment of any tax or duty.
   - Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

b. The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the Bursar.

11. Accuracy

a. The School will endeavour to ensure that all personal data held in relation to workers is accurate. Workers must notify the HR and Compliance Manager of any changes to information held about them. A worker has the right to request that inaccurate information about them is erased.

12. Summary

a. It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

b. A good rule of thumb here is to ask yourself questions such as:
   - Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
   - Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
   - What would be the consequences of my losing or misdirecting this personal data?

c. Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

13. Further information

a. This policy will be reviewed every academic year or sooner if changes to legislation, compliance requirements or good practice dictate.

Appendix 1 – Staff Privacy Notice

In the course of your employment, engagement or other basis of work undertaken for the school, we will collect, use and hold ("process") personal data relating to you as a member of our staff. This makes the school a data controller of your personal information, and this Privacy Notice sets out how we will use that information and what your rights are.

1. Who this document applies to

1.1 Academic and other staff, contractors, peripatetic teachers, casual workers, temps and volunteers who may be employed or engaged by the school to work for it in any capacity, as well as prospective applicants for roles. It also applies to governors.

This notice is not aimed at pupils, or parents of pupils (whether current, past or prospective) or other members of the public, nor does it inform staff how to handle the personal data of the same. This information may be found in the school's Privacy Policy, which provides further details about how personal data will be used by the school, and the staff Data Protection Policy respectively.

Please note that any references to "employment", "staff" etc. in this Notice are not intended to imply or confer any employment rights on non-employees.

2. About this document

2.1 This Staff Privacy Notice explains how the school collects, uses and shares (or "processes") personal data of staff, and your rights in relation to the personal data we hold.

This Privacy Notice also applies in addition to the school's other relevant terms and conditions and policies, including:

- any contract between the school and its staff, such as the terms and conditions of employment, and the Staff Handbook.
- the school's Retention of records policy;
- the school's Safeguarding, Anti-bullying, or Health and safety policies, including as to how concerns or incidents are reported or recorded (both by and about staff); and
- the Digital Strategy policy.

2.2 Please note that your contract with the school, including any document or policy forming a part of your contractual obligations to the school, may in particular be relevant to and supplement the information in this Staff Privacy Notice, to the extent that it will contain details of obligations or rights of the school under contract with you which may require the use of your personal data. However, this Staff Privacy Notice is the primary document applicable to the use of your personal data by the school.

This Staff Privacy Notice also applies alongside any other information the school may provide about particular uses of personal data, for example when collecting data via an online or paper form.

3. How we collect your information

3.1 We may collect your personal data in a number of ways, for example:

- from the information you provide to us before making a job application, for example when you come for an interview;
- when you submit a formal application to work for us, and provide your personal data in application forms and covering letters, etc.; and
- from third parties, for example the Disclosure and Barring Service (DBS) and referees (including your previous or current employers or school), in order to verify details about you and/or your application to work for us.

3.2 More generally, during the course of your employment with us, as a member of staff, we will collect data from or about you, including:

- when you provide or update your contact details;
- when you or another member of staff completes paperwork regarding your performance appraisals;
- in the course of fulfilling your employment (or equivalent) duties more generally, including by filling reports, note taking, or sending emails on school systems;
- in various other ways as you interact with us during your time as a member of staff, and afterwards, where relevant, for the various purposes set out below.

4. The types of information we collect

4.1 We may collect the following types of personal data about you (and your family members and 'next of kin', where relevant):

- contact and communications information, including:
  - your contact details (including email address(es), telephone numbers and postal address(es);
  - contact details (through various means, as above) for your family members and 'next of kin', in which case you confirm that you have the right to pass this information to us for use by us in accordance with this Privacy Notice;
  - records of communications and interactions we have had with you;
- biographical, educational and social information, including:
  - your name, title, gender, nationality and date of birth;
  - your image and likeness, including as captured in photographs taken for work purposes;
  - details of your education and references from your institutions of study;
  - your interests and extra-curricular activities;
- financial information, including:
  - your bank account number(s), name(s) and sort code(s) (used for paying your salary and processing other payments);
  - your tax status (including residence status);
  - information related to pensions, national insurance, or employee benefit schemes;
- work related information, including:
  - details of your work history and references from your previous employer(s);
  - your personal data captured in the work product(s), notes and correspondence you create while employed by or otherwise engaged to work for the school;
  - details of your professional activities and interests;

- your involvement with and membership of sector bodies and professional associations;
- information about your employment and professional life after leaving the school, where relevant (for example, where you have asked us to keep in touch with you);

- and any other information relevant to your employment or other engagement to work for the school.

4.2 Where this is necessary for your employment or other engagement to work for us, we may also collect special categories of data, and information about criminal convictions and offences, including:

- trade union membership, where applicable;
- information concerning your health and medical conditions (for example, where required to monitor and record sickness absences, dietary needs, or to make reasonable adjustments to your working conditions or environment);
- [biometric information, for example where necessary for school security systems];
- information concerning your sexual life or orientation (for example, in the course of investigating complaints made by you or others, for example concerning discrimination); and
- information about certain criminal convictions (for example, where this is necessary for due diligence purposes, or compliance with our legal and regulatory obligations);

4.3 However, this will only be undertaken where and to the extent it is necessary for a lawful purpose in connection with your employment or other engagement to work for the school.

5. The bases for processing your personal data, how that data is used and whom it is shared with

(i) Entering into, or fulfilling, our contract with you

We process your personal data because it is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract, such as a contract of employment or other engagement with us. In this respect, we use your personal data for the following:

- administering job applications and, where relevant, offering you a role with us;
- carrying out due diligence checks on you, whether during the application process for a role with us or during your engagement with us, including by checking references in relation to your education and your employment history;
- once you are employed or engaged by us in any capacity, for the performance of the contract of employment (or other agreement) between you and us;
- to pay you and to administer benefits (including pensions) in connection with your employment or other engagement with us;
- monitoring your attendance and your performance in your work, including in performance appraisals;
- promoting the school to prospective parents and others, including by publishing the work product(s) you create while employed by or otherwise engaged to work for the school;
- for disciplinary purposes, including conducting investigations where required;

- for other administrative purposes, for example to update you about changes to your terms and conditions of employment or engagement, or changes to your pension arrangements;
- for internal record-keeping, including the management of any staff feedback or complaints and incident reporting; and
- for any other reason or purpose set out in your employment or other contract with us.

(ii) Legitimate Interests

We process your personal data because it is necessary for our (or sometimes a third party's) legitimate interests. Our "legitimate interests" include our interests in running the school in a professional, sustainable manner, in accordance with all relevant ethical, educational, charitable, legal and regulatory duties and requirements (whether or not connected directly to data protection law). In this respect, we use your personal data for the following:

- providing you with information about us and what it is like to work for us (where you have asked for this, most obviously before you have made a formal application to work for us);
- for security purposes, including by operating security cameras in various locations on the school's premises;
- to enable relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;
- to provide education services to pupils;
- to safeguard pupils' welfare and provide appropriate pastoral care;
- to carry out or cooperate with any school or external complaints, disciplinary or investigatory process;
- for the purposes of management planning and forecasting, research and statistical analysis;
- in connection with organising events and social engagements for staff;
- making travel arrangements on your behalf, where required;
- contacting you or your family members and 'next of kin' for business continuity purposes, to confirm your absence from work, etc.;
- publishing your image and likeness in connection with your employment or engagement with us;
- to monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's Digital Strategy policy and government guidance such as Keeping Children Safe in Education (KCSIE).

(iii) Legal Obligations

We also process your personal data for our compliance with our legal obligations, notably those in connection with employment, charity law], tax law and accounting, and child welfare. In this respect, we use your personal data for the following:

- to meet our legal obligations (for example, relating to child welfare, social protection, equality, employment, and health and safety);

- for tax and accounting purposes, including transferring personal data to HM Revenue and Customs to ensure that you have paid appropriate amounts of tax, and in respect of any Gift Aid claims, where relevant;
- for the prevention and detection of crime, and in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities.

(iv) Special categories of data

We process special categories of personal data (such as data concerning health, or union membership) or criminal convictions and allegations for the reasons set out below.

We will process this data on the basis that such processing is necessary to carry out obligations and exercise rights (both yours and ours) in relation to your employment.

In particular, we process or may process the following types of special category personal data for the following reasons:

- your physical or mental health or condition(s) in order to record sick leave and take decisions about your fitness for work, or (in emergencies) act on any medical needs you may have;
- recording your racial or ethnic origin in order to monitor our compliance with equal opportunities legislation;
- trade union membership, in connection with your rights as an employee and our obligations as an employer;
- categories of your personal data which are relevant to investigating complaints made by you or others, for example concerning discrimination, bullying or harassment;
- data about any criminal convictions or offences committed by you, for example when conducting criminal background checks with the DBS, or where it is necessary to record or report an allegation (including to police or other authorities, with or without reference to you);

We will process special categories of personal data for lawful reasons only, including because:

- you have given us your explicit consent to do so, in circumstances where consent is appropriate;
- it is necessary to protect your or another person's vital interests, for example, where you have a life-threatening accident or illness in the workplace and we have to process your personal data in order to ensure you receive appropriate medical attention;
- it is necessary for some function in the substantial public interest, including the safeguarding of children or vulnerable people, or as part of a process designed to protect others from malpractice, incompetence or unfitness in a role (or to establish the truth of any such allegations); or
- it is necessary for the establishment, exercise or defence of legal claims, such as where any person has brought a claim or serious complaint against us or you.

(v) Sharing your information with others

For the purposes referred to in this privacy notice and relying on the bases for processing as set out above, we may share your personal data with certain third parties. We may disclose limited personal data (including in limited cases special category or criminal data) to a variety of recipients including:

- other employees, agents and contractors (for example, third parties processing data on our behalf as part of administering payroll services, the provision of benefits including pensions, IT etc. – although this is not sharing your data in a legal sense, as these are considered data processors on our behalf);
- DBS and other relevant authorities and agencies such as the Department for Education, NCTL, the ICO, Charity Commission and the local authority;
- external auditors or inspectors;
- our advisers where it is necessary for us to obtain their advice or assistance, including insurers, lawyers, accountants, or other external consultants;
- third parties and their advisers in the unlikely event that those third parties are acquiring or considering acquiring all or part of our school, or we are reconstituting or setting up some form of joint working or partnership arrangement in the unlikely event that those third parties are acquiring or considering acquiring all or part of our school, or we are reconstituting or setting up some form of joint working or partnership arrangement in the UK or abroad;
- when the school is legally required to do so (by a court order, government body, law enforcement agency or other authority of competent jurisdiction), for example HM Revenue and Customs or police.

We may also share information about you with other employers in the form of a reference, where we consider it appropriate, or if we are required to do so in compliance with our legal obligations.

6. How long your information is kept

6.1 Personal data relating to unsuccessful job applicants is deleted within six months of the end of the application process, except where we have notified you we intend to keep it for longer (and you have not objected).

6.2 For employees, subject to any other notices that we may provide to you, we may retain your personal data for a period of seven years after your contract of employment (or equivalent agreement) has expired or been terminated.

6.3 However, some information may be retained for longer than this, for example incident reports and safeguarding files, in accordance with specific legal requirements. Please see our Retention of Records policy.

7. Your rights

7.1 Please see our Privacy Policy which has details of your rights as a 'data subject', which are the same as if you were any member for the public. You can find out more about your rights under applicable data protection legislation from the Information Commissioner's Office website available at www.ico.org.uk.

8. This notice

8.1 The school will update this Staff Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

9. Contact and complaints

9.1 If you have any queries about this Staff Privacy Notice or how we process your personal data, or if you wish to exercise any of your rights under applicable law, you may contact either the Data Controller (Bursar) or the HR and Compliance Manager or you may refer the matter through the staff grievance procedure which can be found in the Staff Handbook.

9.2 If you are not satisfied with how we are processing your personal data, or how we deal with your complaint, you can make a complaint to the Information Commissioner: www.ico.org.uk. The ICO does recommend you seek to resolve any issues with the data controller initially prior to any referral.

Appendix 2 - Table of suggested retention periods

Type of Record/Document	Suggested[1] 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: e.g. marks / timetables / assignments)
Record of complaints	Where there are no safeguarding concerns – 7 years
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: • Pupil reports • Pupil performance records • Pupil medical records	ALL: 25 years from date of birth (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).
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 NB – please read notice at the top of this note	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates	Certificates not to be kept but a permanent record of the checks being made must be kept.

[1] General basis of suggestion:

Some of these periods will be mandatory legal requirements (e.g. 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.

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 / 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).
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*) [NB specific ambit to be advised by an accountancy expert]	Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place
Tax returns and VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 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.

[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.

Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
Intellectual property records	
Formal documents of title (trademark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, e.g. trademarks); otherwise expiry 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 e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS ***NB this will contain personal data***	
Staff personnel file	Duration of employment plus minimum of 7 years 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	Possibly permanent, depending on nature of scheme
Job application and interview/rejection records (unsuccessful applicants)	Six months
Immigration records	Minimum – 4 years
Health records relating to employees and Employee appraisals or reviews	7 years from end of contract of employment
Single Central Record of employee	Keep a permanent record of all mandatory checks that have been undertaken
Contracts of employment	7 years from effective date of end of contract

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 & data	
Maintenance logs	10 years from date of last entry
Accidents to children[4]	25 years from birth (longer for safeguarding)
Accident at work records (staff)[4]	Minimum – 4 years from date of accident, but review case-by-case where possible
Staff use of hazardous substances [4]	Minimum – 7 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)

[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.