



Applicable to all parties (past and present) with some connection to The National Mathematics and Science College and any associated trusts and/or companies

Purpose

The 2018 Data Protection Act gives individuals the right to understand how their data is used. All who share their data with us should be reassured that we will treat it with respect, ensuring its accuracy, security and use only for the (legitimate and clearly specified) purposes for which it is needed or provided.

The purpose of this Privacy Notice is to ensure that all parties who have any connection with The National Mathematics and Science College (the College) and others whose data we process understand what this means in practice.

Anyone who works for, or acts on behalf of, the College (including staff, volunteers, Members of Board of Governors and service providers) is required to comply with this Privacy Notice and will be subject to suitable training and/or policies commensurate with their role.

Scope

In this Privacy Notice, whenever you see the words 'we', 'us', 'our', 'the College', they apply to everyone collecting, using or processing data on the College's behalf. This includes all members of the College staff, the Governing body, volunteers, and service providers.

The Privacy Notice covers **all personal data** used or processed by the College, notably that of its suppliers, current and prospective staff; its current, past and prospective students; and their parents, carers or guardians (referred to in this policy as "parents"), volunteers working on the College's behalf, and any third parties processing data on the College's behalf. Collectively, we refer to these individuals in the Privacy Notice as the College's community. 'Personal data' means any information relating to an identifiable person who can be directly or indirectly identified through the data.

This Privacy Notice applies alongside any other information the College may provide about a particular use of personal data.

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

- any contract between the College and its staff or the parents of students;
- the College's policy on taking, storing and using images of children;
- the College's safeguarding, pastoral, bullying and health and safety policies, including how concerns or incidents are recorded; and

- the College's IT policies, including its IT Acceptable Use Policy

Responsibility for Data Protection

The College has appointed the Director of Finance and Resources as the Privacy and Compliance Officer who will deal with all requests and enquiries concerning the College's uses of personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and thus with Data Protection Law.

Why the College Needs to Process Personal Data

In order to carry out its ordinary duties, the College needs to process a wide range of personal data about individuals (including current, past and prospective staff, students or parents) as part of its daily operation.

Contractual obligations

The College needs to process personal data in order to fulfil its contractual obligations to its service providers, staff, and parents of its students, for example for making and receiving contractual payments and providing necessary data to pension providers.

Legitimate Interests

Other uses of personal data will be made in accordance with the College's legitimate interests or the legitimate interests of third parties that are key to the effective functioning of the College (e.g. examination boards). This covers the processing of personal data that is necessary for the College to function whilst not outweighing any objection or risks to a data subject's rights and freedoms

The College expects that the following uses will fall within that category of its legitimate interests:

1. For the purposes of student selection, confirming the identity of prospective students and their parents and retaining a record if appropriate for the purposes of future applications or openings;
2. Providing education services including musical education, physical training, career services, and extra-curricular activities to students and monitoring students' progress and educational needs, including where such activities are provided remotely (either temporarily or permanently);
3. Using remote learning platforms as part of this provision of education services;
4. To enable students to take part in national or other assessments, and to publish the results of public examinations or other achievements of students of the College
5. Giving and receive information and references about past, current and prospective students, including those relating to outstanding fees or payment history, to/from any educational institution that the student attended or which they wish to attend; and provide references to potential employers of past students;
6. Safeguarding students' welfare and providing appropriate pastoral care;
7. Monitoring the use of the College's IT and communications systems in accordance with the College's IT Acceptable Use Policy;
8. Enabling relevant authorities to monitor the College's performance and to intervene or assist with incidents as appropriate;
9. Maintaining relationships with alumni and the College community, including direct marketing or fundraising activity (see the section below on Keeping in Touch and Supporting the College);
10. Confirming the identity and background of anyone wishing to make a donation;
11. For the purposes of school management planning and forecasting, research and statistical analysis;

12. To carry out or cooperate with any school or external complaints, disciplinary or investigation process; and
13. Where otherwise reasonably necessary for the College's purposes, including to obtain appropriate professional advice and insurance for the College.

Legal Requirement

The following uses of personal data by the College are required to meet the College's legal obligations:

- Data processing required for tax, diversity and gender pay gap analysis;
- For regulatory record keeping / compliance purposes in respect of immigration requirements, as an employer and/or visa sponsor;
- To take up references prior to engagement of volunteers and staff including but not limited to Disclosure and Barring Service (DBS) applications, "List 99" checks on previous employment references and if applicable overseas police checks;
- To comply with Her Majesty's Revenue and Customs' regulations and those of pension providers;
- To comply with Health and Safety law;
- To comply with local authority instructions.

Consent

Examples of where we do rely on consent are:

- To make use of photographic images of students in college publications, on the College's website and (where appropriate) on the College's social media channels in accordance with the College's policy on taking, storing and using images of children;
- Collecting and using data for certain types of fundraising activity (notably for the use of electronic fundraising in accordance with the Privacy Electronic Communications Regulations).

Where the College is relying on **consent** as a means to process personal data, any person may withdraw this consent at any time.

Types of Personal Data Processed by the College

This will normally include (by way of example):

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- car details (about those who use our car parking facilities);
- bank details and other financial information, e.g. about parents (or others) who pay fees to the College, contractors and staff who need paying etc; In addition, the College may collect any anti-money-laundering information we are required to collect by law;
- past, present and prospective students' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- data in personnel files, including qualifications, employment history, performance appraisal and safeguarding;
- nationality and other immigration status information (e.g. right to work / study), including copies of passport information (retained for booking and during college trips and to comply with immigration sponsor requirements)
- where appropriate, information about individuals' health and welfare;
- contact details for their next of kin;

- references given or received by the College about students, and relevant information provided by previous educational establishments and/or other professionals or organisations working with students;
- correspondence with and concerning staff, students and parents past and present; and
- images of students (and occasionally other individuals) engaging in college activities.

In addition, the College will on occasion need to process **special category personal data** (concerning health, ethnicity, religion, or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required.

These reasons could include:

- To safeguard students' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example for medical advice, for social protection, safeguarding, and cooperation with police or social services, for insurance purposes or to caterers or organisers of college trips who need to be made aware of dietary or medical needs;
- To provide educational services in the context of any special educational needs of a student;
- To provide spiritual education in the context of any religious beliefs;
- In connection with employment of its staff, for example DBS checks, welfare, union membership or pension plans;
- As part of any college or external complaints, disciplinary or investigation process that involves such data, for example if there are Special Educational Needs and Disability (SEND), health or safeguarding elements; or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

How the College Collects Data

Most information is collected from the individual directly (and in the case of students, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

In some cases personal data will be supplied by third parties (for example another school, or other professionals or authorities working with that individual); or collected from publicly available resources.

Data Accuracy and Security

The College will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals should notify the College of any significant changes to important information, such as contact details, held about them.

The College constantly monitors what appropriate technical and organisational steps it must take to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to college systems. All staff and governors are made aware of this policy and their duties under Data Protection Law and receive relevant training.

Who has Access to Personal Data and With Whom the College Shares it

Occasionally, the College will need to share personal information relating to its community with third parties, such as:

- professional advisers (e.g. lawyers, insurers, PR advisers and accountants);
- government authorities (e.g. HMRC, DfE, police or the local authority);
- appropriate regulatory bodies e.g. [Teachers Regulation Agency \(TRA\)](#), the [Independent Schools Inspectorate](#), the Charity Commission or the Information Commissioner and;
- Academic authorities e.g. Awarding Bodies (Examination Boards), those who provide education services (e.g. CEM Centre); Trustees of bursary trust funds.
- appropriate contractors, such as visiting music teachers;
- organisations set up to help establish and maintain relationships between the College and its community
- web developers: e.g. the College database (iSAMS) is stored in the cloud
- a third-party caterer with whom personal data may sometimes be shared;
- college photographers
- stage 3 complaints panels, which will include independent panel members;
- third parties and their advisers in the event of a possible or actual sale, merger or other restructuring of the College; and
- government authorities (e.g. HMRC, DfE, CAFCASS, police, Home Office, a relevant public health / NHS body and / or local authority) and/or appropriate regulatory bodies (e.g. the [Teaching Regulation Agency](#), the [Independent Schools Inspectorate](#), the [Charity Commission](#));

In accordance with Data Protection Law, this type of external data processing is always subject to contractual assurances that personal data will be kept securely and used only in accordance with the College's specific directions.

We will not however share personal information about our workforce with anyone without receiving the explicit consent to do so unless the law and/or our policies require us to do so.

For the most part, personal data collected by the College will remain within the College, and will be accessed and processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis).

Sensitive Medical and Safeguarding Data

Particularly strict rules of access apply in the context of:

- **Medical data.** The College needs to process such information to comply with statutory duties and to keep students and others safe, but the College will ensure only authorised staff can access information on a need-to-know basis. This may include wider dissemination if needed for college trips or for catering purposes. Express consent will be sought where appropriate.
However, a certain amount of any SEND students' relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the student requires.
- **Safeguarding data.** Under duties imposed by law and statutory guidance (including 'Keeping Children Safe in Education or KCSIE) the College is required to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This is likely to include file notes on personnel or safeguarding files, and in some

cases referrals to relevant authorities such as the Local Authority Designated Officer (LADO) or police. KCSIE also requires that, whenever a child leaves the College to join another school or college, his or her child protection file is promptly provided to the new organisation. The College will retain a copy in accordance with its retention policy for material related to safeguarding matters.

For further information about this, please view the College's Safeguarding Policy.

How Long we Keep Personal Data

The appendix at the end of the document sets out the duration and rationale for data retention. The principles of data retention underlying this are that:

- the College will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason, including contractual obligations;
- data is retained in line with statutory duties and government guidance relating to Schools, including for safeguarding;
- the retention of data will take on board the disclosure requirements for potential future litigation;
- data retention, confidentiality and privacy will be fully in line with the GDPR.

Typically, the legal recommendation for how long to keep ordinary staff and student personnel files is up to 7 years following departure from the College. However, incident reports and safeguarding files need to be kept much longer, in accordance with specific legal requirements. In particular, the Independent Inquiry into Child Sexual Abuse (IICSA) stipulates that, until further notice, all staff files should be retained for 50 years after leaving.

A limited and reasonable amount of information will be retained for archiving purposes, and even where you have requested we no longer keep in touch with you, we will need to keep a record of the fact in order to fulfil your wishes (called a "suppression record").

If you have any specific queries about how our retention policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the Director of Finance and Resources on finance@natmatsci.ac.uk. However, please bear in mind that the College will often have lawful and necessary reasons to retain personal data even following such a request.

Keeping in Touch and Supporting the College

The College and/or any relevant other organisation will use the contact details of parents, alumni and other members of the College community to keep them updated about the activities of the College, or alumni and parent events of interest, including by sending updates and newsletters, by email and by post. Given that this is covered by the College's Legitimate Interests, the College will, unless the relevant individual objects:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships between the College and its community
- Contact parents and/or alumni (including via the organisations above) by post, telephone and email in order to promote and raise funds for the College and, where appropriate, other worthy causes;

Should you wish to limit or object to any such use, or would like further information about them, please contact the Director of Finance and Resources in writing. You always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the College is nonetheless likely to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

Your Rights

Individuals (both students and parents) have various rights under Data Protection Law to access and understand their own personal data held and processed by the College, and in some cases ask for it to be erased or amended, or to have it transferred elsewhere, or for the College to stop processing it – but subject to certain exemptions and limitations.

The College will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits (which is generally one month, but actually fulfilling more complex or multiple requests, e.g. those involving third party information, may take 1-2 months longer). Individuals (both students and parents) have various rights under Data Protection Law to access and understand their own personal data held and processed by the College, and in some cases ask for it to be erased or amended, or to have it transferred elsewhere, or for the College to stop processing it – but subject to certain exemptions and limitations.

You have the following rights:

- to obtain access to, and copies of, the personal data that we hold about you;
- to be informed about how your personal information is collected, used, shared and retained;
- to receive from us the personal data we hold about you which you have provided to us, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller;
- to object, on grounds relating to your particular situation, to any of our particular processing activities where you feel this has a disproportionate impact on your rights.
- to require us correct any inaccuracies in your personal data;
- in some cases to ask for it to be erased;
- or amended or have it transferred to others, or for the College to stop processing it – but subject to certain exemptions and limitations.
- where the information is held on the basis of consent to request that we restrict our data processing activities (and, where our processing is based on your consent, you may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal);

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the Director of Finance and Resources.

Note that the right of data access applies only to your own personal data, and does **not** include:

- Information which identifies other individuals. (Parents need to be aware this may include their own children, in certain limited situations – please see further below.)

Information which is subject to legal privilege (for example legal advice given to or sought by the College, or documents prepared in connection with a legal action or where a duty of confidence is owed by a legal adviser).

- Student examination scripts (or other information consisting solely of student test answers), or examination or other test marks ahead of any ordinary publication). These exemptions necessarily apply also in the context of teacher-assessed grades, where required in the absence of formal public examinations due to pandemic conditions
- Confidential references given by the College itself for the purposes of the education, training or employment of any individual.

Students can make subject access requests for their own personal data, provided that, in the reasonable opinion of the College, they have sufficient maturity to understand the request they are making. Students at the College, given their age, are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home.

A student of any age may ask a parent or other representative to make a subject access request on his/her behalf. The College may also consider there are lawful grounds for sharing with or without reference to that student. Parents will in general receive educational and pastoral updates about their children, in accordance with the Parent Contract. Where parents are separated, the College will in most cases aim to provide the same information to each person with parental responsibility, but may need to factor in all the circumstances including the express wishes of the child. All information requests from, on behalf of, or concerning students – whether made under subject access or simply as an incidental request – will therefore be considered on a case-by-case basis.

While a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger students, the law still considers the information in question to be the child's. It may in some cases be necessary or appropriate – given the nature of the processing in question, and the student's age and understanding – to seek the student's consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances. Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the College may be under an obligation to maintain confidentiality unless, in the College's opinion, there is a good reason to do otherwise; for example where the College believes disclosure will be in the best interests of the student or other students, or if required by law.

Students are required to respect the personal data and privacy of others, and to comply with the College's IT Acceptable Use Policy and the College rules. Staff are under professional duties to do the same covered under the relevant staff policies.

It should be clearly understood that the rules on subject access are not the sole basis on which information requests are handled. Parents may not have a statutory right to information, but they and others will often have a legitimate interest or expectation in receiving certain information about students without their consent. The College may consider that there are lawful grounds for sharing, with or without reference to that student.

All information requests from, on behalf of, or concerning students – whether made under subject access or simply as an incidental request – will therefore be considered on a case-by-case basis.

Summary of Rights

The rights under Data Protection Law belong to the individual to whom the data relates. However, the College will often rely on parental authority or notice for the necessary ways it processes personal data relating to students – for example, under the parent contract, or via a form. Parents and students should be aware that this is not necessarily the same as the College relying on strict consent (see section on Consent in “Why the College Needs to Process Personal Data”).

Where consent is required, it may in some cases be necessary or appropriate – given the nature of the processing in question, and the student's age and understanding – to seek the student's consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances.

In general, the College will assume that students' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the student's activities, progress and behaviour, and in the interests of the student's welfare. That is unless, in the College's opinion, there is a good reason to do otherwise.

However, where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the College may be under an obligation to maintain confidentiality unless, in the College's opinion, there is a good reason to do otherwise; for example where the College believes disclosure will be in the best interests of the student or other students, or if required by law.

Amendments to This Policy

The College will update this 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.

Queries, Concerns and Complaints

Any comments or queries on this policy should be directed to the Director of Finance and Resources by emailing finance@natmatsci.ac.uk

If an individual believes that the College has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the College complaints procedure and should also notify the Principal. You can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the College before involving the regulator.

Further Information

Any comments or queries on this policy should be directed to the Director of Finance and Resources using the following contact details finance@natmatsci.ac.uk. The College's Director of Finance and Resources acts as Privacy and Compliance Officer responsible for:

- following up requests, including on rights of access and amendment;

- responding to enquiries concerning the College's uses of personal data; and
- taking the lead on ensuring that all personal data is processed in compliance with this policy and the GDPR.

Further information on the GDPR is also available on the website of the Information Commissioners' Office (ICO):
<https://ico.org.uk>.

Director of Finance and Resources

Chris Voisey

Date of Review: March 2024

Date of Next Review: March 2026

Appendix: Data Retention

This policy sets out the minimum periods of retention of the personal data that we process. Schools will generally 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. However, 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 General Data Protection Regulations and associated legislation.

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

Child protection and document retention

In the light of the Independent Inquiry into Child Sexual Abuse and various high-profile safeguarding cases, all independent schools are aware of the emphasis currently being placed on long-term, lifetime or even indefinite keeping of full records related to incident reporting. Regardless of suggested retention timescales set out below, The National Mathematics and Science College may at its discretion extend this rule to any and/or all personnel and students files on a 'safety first' basis.

These guidelines have been drafted in full awareness of these considerations. Data protection issues should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding

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 students. Some of this material, but not all, will contain personal data of individuals as defined in the GDPR.

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.

Both paper and digital records will be stored securely and all appropriate measures taken to ensure the security of the data at all times.

Secure disposal of documents

When data is to be destroyed, this may be carried out by an appropriately licenced third party, with whom an appropriate Data Processing Agreement is in place.

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

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

Where third party disposal experts are used they will be subject to adequate contractual obligations to the College to process and dispose of the information confidentially and securely.

Timescales for retention

Except where there is a specific statutory obligation to destroy records, it is misleading to treat these suggestions as prescriptive 'time-limits'. Figures given are not intended as a substitute to exercising thought and judgment, or taking specific advice, depending on the circumstances.

The figures suggested in this table are, in most cases, guides as to what are periods of reasonable necessity that could be defensible if challenged. Case by case decision making for documents would in theory be ideal, but in reality practical considerations mean that regular 'pruning' of records may not be an acceptable use of school resources. It is therefore accepted that sometimes a more systemic or broad-brush approach is necessary.

TABLE OF SUGGESTED RETENTION PERIODS

Type of Record/Document	<u>Suggested</u> Retention Period
EMAILS ON SERVER <ul style="list-style-type: none"> • Student email account • Staff emails 	Delete upon leaving college, or within one year Routine deletion of historic emails after 2 – 3 years and delete account within 1 year of leaving college
COLLEGE-SPECIFIC RECORDS <ul style="list-style-type: none"> • Registration documents of College • Attendance Register • Minutes of Governors' meetings • Annual curriculum 	Permanent (or until closure of the College) 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 STUDENT RECORDS <ul style="list-style-type: none"> • Admissions: application forms, assessments, records of decisions • Student immigration records • Examination results (external or internal) • Student file including: <ul style="list-style-type: none"> ▪ Reports ▪ Performance records ▪ Medical records <p>Special educational needs records (<i>to be risk assessed individually</i>)</p>	<p><i>NB – this will generally be personal data</i></p> <p>25 years from date of birth (or, if student not admitted, up to 7 years from that decision). Duration of student sponsorship plus minimum 1 year - 7 years from student leaving college</p> <p>ALL: 25 years from date of birth (subject where relevant to safeguarding considerations). Any material which may be relevant to potential claims should be kept for the lifetime of the student.</p> <p>Date of birth plus up to 35 years (risk assessed)</p>

<p>SAFEGUARDING</p> <ul style="list-style-type: none"> • Policies and procedures • DBS disclosure certificates (if held) • Accident / Incident reporting • Child Protection files • Video recordings of meetings 	<p>Keep a permanent record of historic policies</p> <p><u>No longer than 6 months</u> from decision on recruitment, unless police specifically consulted – but a record of the checks being made must be kept on the SCR/Personnel file, but not the certificate itself.</p> <p>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.</p> <p>If a referral has been made / social care have been involved or child has been subject of a multi-agency plan, or there is a risk of future claims – indefinitely.</p> <p>Where e.g. one on one meetings of classes, counselling or application interviews are recorded for safeguarding purposes, a shorter term retention policy is acceptable based on the DSL's view of how quickly a concern will be likely to be raised (eg 3-6 months or immediately upon DSL review)</p>
<p>CORPORATE RECORDS (where applicable)</p> <ul style="list-style-type: none"> • Certificates of Incorporation • Minutes, Notes and Resolutions of Boards or Management Meetings • Shareholder resolutions • Register of Members/Shareholders • Annual reports 	<p><i>e.g. where schools have trading arms</i></p> <p>Permanent (or until dissolution of the company)</p> <p>Minimum – 10 years</p> <p>Minimum – 10 years</p> <p>Permanent (minimum 10 years for ex-members/shareholders)</p> <p>Minimum – 6 years</p>

<p>ACCOUNTING RECORDS</p> <ul style="list-style-type: none"> Accounting records (<i>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</i>) [NB <u>specific ambit to be advised by an accountancy expert</u>] Tax returns VAT returns Budget and internal financial reports 	<p>Minimum – 6 years for private UK companies (except where still necessary for tax returns) 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</p> <p>Minimum – 6 years</p> <p>Minimum – 6 years</p> <p>Minimum – 3 years</p>
<p>CONTRACTS AND AGREEMENTS</p> <ul style="list-style-type: none"> Signed or final/concluded agreements (<i>plus any signed or final/concluded variations or amendments</i>) Deeds (or contracts under seal) 	<p>Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later</p> <p>Minimum – 13 years from completion of contractual obligation or term of agreement</p>
<p>INTELLECTUAL PROPERTY RECORDS</p> <ul style="list-style-type: none"> Formal documents of title (trademark or registered design certificates; patent or utility model certificates) Assignments of intellectual property to or from the College IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents) 	<p>Permanent (in the case of any right which can be permanently extended, eg trademarks); otherwise expiry of right plus minimum of 7 years.</p> <p>As above in relation to contracts (7 years) or, where applicable, deeds (13 years).</p> <p>Minimum – 7 years from completion of contractual obligation concerned or term of agreement</p>
<p>EMPLOYEE / PERSONNEL RECORDS</p> <ul style="list-style-type: none"> Single Central Record of employees Contracts of employment 	<p><i>NB these records will contain personal data</i></p> <p>Keep a permanent record of all mandatory checks that have been undertaken (but do not keep DBS certificate itself: 6 months as above)</p> <p>7 years from effective date of end of contract.</p>

<ul style="list-style-type: none"> Employee appraisals or reviews Staff personnel file 	<p>Duration of employment plus minimum of 7 years As above, but do not delete any information which may be relevant to <u>historic safeguarding claims</u>.</p>
<ul style="list-style-type: none"> Payroll, salary, maternity pay records Pension or other benefit schedule records 	<p>Minimum – 6 years</p> <p>Possibly permanent, depending on nature of scheme</p>
<ul style="list-style-type: none"> Job application and interview/rejection records (unsuccessful applicants) Staff Immigration records 	<p>Minimum 3 months but no more than 1 year</p> <p>Minimum 2 years from end of employment</p>
<ul style="list-style-type: none"> Worker Sponsor Records Health records relating to employees Low level concerns records about adults (where applicable and under a school policy) 	<p>Minimum 1 year from end of employment</p> <p>7 years from end of employment</p> <p>Regular review recommended in order to justify longer term retention as part of safeguarding files.</p>
<p>INSURANCE RECORDS</p> <ul style="list-style-type: none"> Insurance policies (will vary – private, public, professional indemnity) Correspondence related to claims/renewals/notification re: insurance 	<p>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.</p> <p>Minimum – 7 years (depending on what the policy covers and whether e.g. historical claims could be made)</p>
<p>ENVIRONMENTAL & HEALTH RECORDS</p> <ul style="list-style-type: none"> Maintenance logs Accidents to children Accident at work records (staff) Staff use of hazardous substances 	<p>10 years from date of last entry</p> <p>25 years from birth (longer for safeguarding incident)</p> <p>Minimum – 4 years from date of accident, but review case-by-case where possible</p> <p>Minimum – 7 years from end of date of use</p>
<ul style="list-style-type: none"> Article 30 GDPR records of processing activity, data breach records, impact assessments 	<p>No limit (as long as no personal data held) but must be kept up to date, accurate and relevant</p>