North London Collegiate School

Founded 1850

DATA PROTECTION POLICY

Policy Lead	Chief Operating Officer
Reviewed By	Chief Operating Officer, Director of IT & Estates Director
Mid Review Completed	20th October 2023
Authorised By	Senior Team
Date of Authorisation	20th October 2023
Date of Next Review	April 2024
Governing Body Committee with oversight	Pastoral, Safeguarding and Compliance Committee

Contents

1. Introduction

1.1 North London Collegiate School (the School) processes large amounts of "personal data" about members of the School community. Under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act (2018) (DPA), the School must process such personal data "fairly". This includes explaining how personal data will be held and used by the School. This policy is intended to help meet that legal requirement.

1.2 It should be noted, from the outset, that data protection should always take second place to safeguarding and child protection. If there is a potential conflict between the two competing requirements, the welfare of the child is paramount. For further information, see HM Government's non-statutory guidance Information sharing: Advice for practitioners providing safeguarding services to children, young people and carers (July 2018).

1.3 This is a whole school policy which applies from EYFS to sixth form.

1.4 This policy must be read in conjunction with the following which are available on the School website:

- Procedure in the event of a personal data breach (internal document)
- Subject Access Request procedure (internal document)
- Exams Subject Access Request procedure (internal document)
- Code of Conduct for Staff (internal document)
- Data Retention Policy (internal document)
- Information Security policy (internal document)
- Privacy Notices

- Recruitment, Selection and Disclosure policy
- Terms and Conditions

1.5 This policy is available on the School website.

1.6 Copies of the above policies are held at the Senior School Office for consultation by parents. You may also email the School at Office@nlcs.org.uk to request hard copies which can be made available in large print or other accessible format if required.

2. Aims and objectives

2.1 This policy aims to provide information about how the School will use or "process" personal data about individuals including current, past and prospective pupils; and their parents, carers or guardians - referred to in this policy as "parents", staff and visitors.

2.2 The School is committed to protecting the personal data it processes. As part of this commitment the School publishes privacy notices on its website, which explains how the School collects, stores and handles personal data. This policy should be read in conjunction with the School's privacy notices (a parent privacy notice for the whole school, a pupil privacy notice for parents of junior school pupils, a pupil privacy notice for senior school pupils, a privacy notice for staff and a privacy notice for fundraising and development). This policy applies in addition to the School's Terms and Conditions, and any other information the School may provide about a particular use of personal data.

3. Statutory framework

3.1 This policy complies with the following:

- General Data Protection Regulation (EU 2016/679)
- Data Protection Act 2018
- Privacy and Electronic Communications (EC Directive) Regulations (2003),
- Protection of Freedoms Act 2012
- Information Commissioner's Office (ICO) relevant guidance and practice notes namely:
    - CCTV Code of Practice
    - Guidance on Direct Marketing

4. Scope and responsibilities

4.1 This policy and associated procedures apply to anyone who works for or acts on behalf of the School including but not limited to staff, supply staff, volunteers, Governors and service providers.

4.2 In accordance with the DPA and UK GDPR, the School has notified the ICO of its processing activities. The school's ICO registration number is Z4994269 and its registered address is Canons Drive, Edgware, Middlesex, HA8 7RJ.

4.3 Whilst the School is the Data Controller, the School's Chief Operating Officer is the 'Data Protection Lead', who will endeavour to ensure that all personal data is processed in compliance with the UK GDPR.

5. Definitions

5.1 For the purposes of the UK GDPR:

Biometric Data – any personal data relating to the physical, physiological or behavioural characteristics of an individual which allows their unique identification.

Consent – freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data.

Data Concerning Health – any personal data related to the physical or mental health of an individual or the provision of health services to them.

Data Controller – the entity that determines the purposes, conditions and means of processing of personal data.

Data Erasure – also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data and potentially have third parties cease processing of the data.

Data Portability – the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

Data Protection Impact Assessments (DPIAs) – tool to help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

Data Processor – the entity that processes data on behalf of the Data Controller.

Data Subject – a natural person whose personal data is processed by a controller or processor.

Encrypted Data – personal data that is protected through technological measures to ensure that the data is only accessible by those with specified access.

Personal Data – any information related to a natural person or data subject, that can be used directly or indirectly to identify the person.

Personal Data Breach – a breach of security leading to the accidental or unlawful access to, destruction, misuse etc. of personal data.

Privacy by Design – a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

Processing – any operation performed on personal data, whether or not by automated means, including collection, use, recording etc.

Pseudonymisation – substitutes the identity of the data subject in such a way that additional information is required to re-identify the data subject.

Right to be forgotten – also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

Right to Access/Subject Access Request – entitles the data subject to have access to, and information about, the personal data that a controller has concerning them.

Special Categories of Personal Data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Supervisory Authority – The Information Commissioner's Office (ICO) is the Supervisory Authority for the United Kingdom.

6. The principles

6.1 There are seven principles of data protection in the UK GDPR. These principles give people specific rights in relation to their personal data and place certain obligations on those organisations that are responsible for processing it.

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

6.2 The School shall, so far as is reasonably practicable, comply with the principles contained in the UK GDPR to ensure all personal data is:

- processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regards to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality');
- The controller shall be responsible for, and be able to demonstrate compliance with, the above data protection principles ('accountability').

7. Types of personal data processed by the school

7.1 The School may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including 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);
- occupational details
- bank details and other financial information, e.g. about parents who pay fees to the School;
- bursary related information
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the School about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and
- images of pupils engaging in School activities (as set out in the School's Code of Conduct for Staff on taking, storing and using images of children), and images captured by the School's CCTV system.
- Generally, the School receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another School, or other professionals or authorities working with that individual), or collected from publicly available resources.

7.2 In addition, the School may need to process "special categories of personal data" concerning health, religion, biometrics etc. or criminal records information such as when conducting Disclosure and Barring Service (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. Further details can be found in the applicable Privacy Notice available on the School website.

8. Use of personal data by the school

8.1 The School will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents;
- To provide education services (including SEND), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumnae and the School community;
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the School's performance;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School;
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of School trips;
- To monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's Digital Safety policies';
- To make use of photographic images of pupils in School publications, on the School website and where appropriate on the School's social media channels in accordance with the School's policy on taking, storing and using images of children;
- For security purposes, and for regulatory and legal purposes (for example, child protection and health and safety) and to comply with its legal obligations; and
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

9. Individual rights

9.1 The UK GDPR provides the following rights for individuals (including children):

The right to be informed: the School provides privacy notices which ensure transparency of processing, by setting out how the School uses personal data.

The right of access: individuals have the right to access their personal data and supplementary information by making a 'Subject Access Request' (see Section 7). The right of access allows individuals to be aware of and verify the lawfulness of the processing.

The right to rectification: individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

The right to erasure/the right to be forgotten: this right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to restrict processing: individuals have a right to 'block' or suppress processing of personal data under certain circumstances. For example, where an individual contests the accuracy of the personal data, where an individual has objected to the processing, when processing is unlawful and the individual opposes erasure and requests restriction instead etc.

The right to data portability: allows individuals to obtain and reuse their personal data for their own purposes across different services.

The right to object: individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Rights in relation to automated decision making and profiling: the UK GDPR has provisions on:

- automated individual decision-making i.e., making a decision solely by automated means without any human involvement; and
- profiling i.e., automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.

For detailed information on the above rights please go to:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/individual-rights/

9.2 Individuals wishing to exercise individual rights should write to the Data Protection Lead at the School address, or via email, at dataprotection@nlcs.org.uk setting out which right/s they wish to exercise and the reasons for doing so. The School will provide a written response and/or where applicable will action the request within one month of receipt of the written application.

10. Rights of access to personal data ("Subject Access Request")

10.1 Under the UK GDPR, individuals have the right to obtain:

- confirmation from the School that their data is being processed;
- access to their personal data (not whole documents); and
- certain other supplementary information, for example, the purposes of the processing, the categories of personal data concerned, to whom the personal data has been or will be disclosed etc.

10.2 Any individual wishing to access their personal data i.e., making a subject access request can speak to the School's Data Protection Lead, put their request in writing

to the Data Protection Lead at the School address, or email the Data Protection Lead at: dataprotection@nlcs.org.uk

10.3 Any individual wishing to access their *exams* related personal data during term time can speak to the Examinations Secretary, put their request in writing to the Examinations Secretary at the School address, or email the Examinations Secretary at: SBurkett@nlcs.org.uk During the holidays, individuals should contact the Office Manager at dataprotection@nlcs.org.uk with such requests.

10.4 The School will verify the identity of the individual making the subject access request using reasonable means. The School may request a valid form of id e.g., copy of passport or driving licence and/or proof of address etc.

10.5 The School will endeavour to respond to subject access requests as soon as is reasonably practicable, and at the latest within one calendar month of receipt of the request. If the subject access request is complex the School can extend the period of compliance by a further two months. The individual making the subject access request will be informed of the extension within one month of the receipt of the request, and will be provided with an explanation as to why the extension is necessary.

10.6 The School will provide this information free of charge however, a reasonable fee may be charged where the request is manifestly unfounded or excessive, particularly if it is repetitive, and where requests are made for further copies of the same information.

10.7 Where the School processes a large quantity of information about an individual, the UK GDPR permits the School to ask the individual making a subject access request to specify the information their request relates to. The School will be greatly assisted in dealing with such requests if individuals are able to provide a rationale for making the request.

10.8 The School is entitled to refuse to respond to such requests where requests are manifestly unfounded or excessive, particularly if it is repetitive. The individual making the request will, without undue delay and at the latest within one month of the receipt of the subject access request, be provided with an explanation regarding the reason/s for refusal. The individual will also be informed of their right to complain to the supervisory authority i.e., the ICO and to a judicial remedy.

10.9 A subject access request only provides access to the individual's own personal data. This is widely defined to include anything that relates to an identifiable, living individual which means it includes initials, nicknames, job titles etc.

10.10 Where personal data about the person making a subject access request also constitutes personal data about another person (a third party), the School is not obliged to disclose this mixed data in response to the subject access request unless either (a) the third party has consented or (b) it is reasonable, taking into account all the relevant circumstances, to disclose without consent. Otherwise, factors will include the third party's views, any harm or distress that may come to the third party, and the third party's expectations of confidentiality however, the School will disclose

as much of the requester's personal data as it can without unreasonably identifying the third party.

10.11 Under the Data Protection Act 2018, if the third party is a teacher or other employee of a school, the school cannot rely on the mixed personal data exemption in order to withhold personal data i.e., teachers and other school employees are not covered by the mixed personal data exemption. The School is aware that it will always be assumed reasonable to disclose where that other person is a social worker or education worker.

11. Whose rights

11.1 The rights belong to the individual to whom the data relates. However, the School will in most cases rely on parental consent to process personal data relating to pupils (if consent is required) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they may not be consulted.

11.2 In general, the School will assume that pupils consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the School's opinion, there is a good reason to do otherwise.

11.3 However, where a pupil 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 School will maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; for example where the School believes disclosure will be in the best interests of the pupil or other pupils.

11.4 Pupils are required to respect the personal data and privacy of others, and to comply with the School's Digital Safety Policy for Pupils and the School Rules.

12. Keeping in touch and supporting the school

12.1 The School will use the contact details of parents, alumnae and other members of the School community to keep them updated about the activities of the School, including by sending updates and newsletters by email and post, and will only do this where the School is allowed to do so under data protection law.

12.2 Unless the relevant individual objects, the School may also:

- contact parents and/or alumnae in order to promote and raise funds for the School;
- pass on parents and/or alumnae details to other parents and/or alumnae but only once prior written permission to do so has been obtained.

12.3 Should you wish to limit or object to any such use or would like further information about them, please email the Development Manager at GMann@nlcs.org.uk

13. Data accuracy and security

13.1 The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the School in writing of any changes to information held about them.

13.2 An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations) and may do so by contacting the Data Protection Lead, in writing at the School address, or via email, at dataprotection@nlcs.org.uk

13.3 The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals. All staff will be made aware of this policy and their duties under the UK GDPR.

14. Reporting data breaches

14.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

14.2 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In brief, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

14.3 In the event of a breach or suspected breach the member of staff must immediately inform the Data Protection Lead via email at dataprotection@nlcs.org.uk, and their line manager, providing as much information as possible. The Data Protection Lead will establish whether a personal data breach has occurred and, if so, promptly take the necessary steps to address it.

14.4 If a personal data breach has occurred the Data Protection Lead will establish the likelihood and severity of the resulting risk to the individual/s rights and freedoms. If it is deemed that there will be a risk, the Data Protection Lead will notify the Information Commissioner's Office (ICO), without undue delay, and not later than 72 hours after having become aware of the breach. If it is unlikely that there will be a risk to individual/s rights and freedoms the breach will not be reported to the ICO.

14.5 If there is a likelihood of a *high* risk to the individual/s rights and freedoms the Data Protection Lead will also report the breach, without undue delay, to the individual/s who have been affected. Examples of high-risk situations include, amongst other things, individual/s suffering discrimination, damage to reputation, financial loss, other significant economic or social disadvantage as a consequence of the breach.

14.6 The Data Protection Lead will also notify the Designated Safeguarding Lead if the breach or suspected breach relates to pupil data.

15. Data retention and storage guidelines

15.1 In these guidelines, "record" means any document or item of data which contains evidence or information relating to the School, its staff or pupils. Some of this material will contain personal data of individuals as defined in the UK 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.

16. Storage of records

Digital records:

16.1 Digital records can be lost or misappropriated in huge quantities very quickly. Access to special categories of personal data, or any large quantity of data, should as a minimum be password protected and held on a limited number of devices only, with passwords provided on a need to know basis and regularly changed.

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

16.3 Staff should bear in mind that documents and records, including emails, may be disclosable due to litigation, investigation or the receipt of a subject access request, and therefore should be accurate and professional.

Paper records:

16.4 Paper records are only classed as personal data if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category but a merely chronological file of correspondence may well not. Where personal information is contained on print-outs taken from electronic files, the data has already been processed by the School and falls within the UK GDPR. Paper records should be stored in a secure, dry, cool and reasonably ventilated area.

Archiving and the destruction of records:

16.5 Staff given specific responsibility for the management of records must ensure, as a minimum, the following:

- That records, whether electronic or hard copy, are stored securely, including if possible, with encryption, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable;

- That important records, and large or sensitive personal databases, are not taken home or, in respect of digital data, carried or kept on portable devices unless absolutely necessary;

- Back-ups or migration should be approached in line with general School policy such as professional storage solutions or IT systems and not individual ad hoc action;

- That reviews are conducted on a regular basis, in line with the guidance below, to ensure all information being kept is still relevant and, in the case of personal data, necessary for the purposes for which it is held (and if so, that it is accurate and up to date) and;

- That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely with no risk of the re-use or disclosure, or reconstruction, of any records or information contained in them.

17. 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)
• Admission and Attendance Registers'	3 years after the end of the school year in question
• Minutes of Governors' meetings	Permanent
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. 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)	Indefinitely
• Pupil file including: o Pupil reports o Pupil performance 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.)

o Pupil medical records • 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)
<u>SAFEGUARDING</u> • Policies and procedures • Accident / Incident reporting • Child Protection files	Keep a permanent record of historic policies 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] 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).

<u>CORPORATE RECORDS (where applicable)</u> • Certificates of Incorporation • Shareholder resolutions • Register of Members/Shareholders • Annual reports	**e.g., *where schools have trading arms*** Permanent (or until dissolution of the company) Minimum – 10 years Permanent (minimum 10 years for ex-members/shareholders) Minimum – 6 years
<u>GOVERNORS RECORDS</u> • Minutes, Notes and Resolutions of Boards Meetings	Permanent

• Register of Directors	Permanent
• Declaration of Interest forms	Permanent
ACCOUNTING RECORDS [3]	
• Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*)	Minimum – 3 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
• Tax returns	Minimum – 6 years
• 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*)	Kept indefinitely
• Deeds (or contracts under seal)	Kept indefinitely
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, e.g., trade marks); 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***
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above)
• Contracts of employment	7 years from effective date of end of contract
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims.
• Payroll, salary, maternity pay records	Minimum – 6 years
• Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme
• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
• Immigration records	Minimum – 4 years
• Health records relating to employees	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 AND DATA	
• Maintenance logs	10 years from date of last entry
• Accidents to children [4]	25 years from birth (unless safeguarding incident)

• 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)

FOOTNOTES:

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.

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 (e.g. every 6 years) in place.*

3. *Retention period for tax purposes should <u>always</u> be made by reference to specific legal or accountancy advice.*

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

Please see the School's Data Retention Policy for further details of the School's approach to reviewing and destroying records.

18. CCTV

18.1 The Closed-Circuit Television System (the CCTV System) is administered and managed by the School, who act as the Data Controller.

18.2 All fixed cameras are in plain sight on the School premises and the School does not routinely use CCTV for covert monitoring or monitoring of private property outside the School grounds.

18.3 The School's purposes of using the CCTV System are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

19. Objectives of the system

- To protect pupils, staff, volunteers, visitors and members of the public with regard to their personal safety
- To protect the School buildings and equipment, and the personal property of pupils, staff, volunteers, visitors and members of the public
- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders
- To monitor the security and integrity of the School site and deliveries and arrivals
- To monitor staff and contractors when carrying out work duties
- To monitor and uphold discipline among pupils in line with the School Rules, which are available to parents and pupils on request

20. Positioning

20.1 Locations have been selected, both inside and out, that the School reasonably believes require monitoring to address the stated objectives.

20.2 Adequate signage has been placed in prominent positions to inform staff and pupils that they are entering a monitored area.

20.3 No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.

20.4 No images of public spaces will be captured except to a limited extent at site entrances.

21. Maintenance

21.1 The CCTV System will be operational 24 hours a day, every day of the year. The Estates Manager will check and confirm that the CCTV System is properly recording and that cameras are functioning correctly, on a regular basis.

21.2 The CCTV System is checked weekly by the School Keepers and serviced no less than annually.

22. Supervision of the system

22.1 The overall responsibility for the CCTV system lies with the Estates Director.

22.2 Staff authorised by the School to conduct routine supervision of the CCTV System may include the School Keepers, supervisors at Canons sports centre and relevant staff on duty.

22.3 Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

23. Storage of data

23.1 The day-to-day management of images will be the responsibility of the Estates Manager or such suitable person as the Estates Manager shall appoint in his absence.

23.2 Every camera on the School site has a different retention period depending on what is in picture, lighting conditions and more. Some cameras are as low as 7 days retention, some as much as 30 days. All cameras are set to expire footage older than 30 days unless the School considers it reasonably necessary for the pursuit of the objectives outlined above, or unless directed by an appropriate third party such as the police or local authority.

23.3 Where such data is retained, it will be retained in accordance with the UK GDPR and this policy. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system log book.

24. Access to images

24.1 Access to stored CCTV images will only be given to authorised persons, under the supervision of the Estates Director, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).

24.2 Individuals also have the right to access personal data the School holds on them, including information held on the CCTV System, if it has been kept. The School will require specific details including at least time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

24.3 The Estates Director must satisfy himself of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the Estates Director may authorise access to CCTV images:

- Where required to do so by the Headmistress, the police or a relevant statutory authority;
- To make a report regarding suspected criminal behaviour;
- To enable the Designated Safeguarding Lead or their appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;
- To assist the School in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the School's management of a particular incident;
- To data subjects (or their legal representatives) pursuant to a subject access request;
- To the School's insurance company where required in order to pursue a claim for damage done to insured property; or
- In any other circumstances required under law or regulation.

24.4 Where images are disclosed a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

24.5 Where images are provided to third parties, wherever practicable, steps will be taken to obscure images of non-relevant individuals.

25. Other CCTV systems

25.1 The School does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this in line with the objectives of the School's own CCTV policy and/or its School Rules.

26. Queries and complaints

26.1 Any comments or queries on this policy, or in relation to the School's CCTV System, should be referred to the Data Protection Lead at the School address, or via email, at: dataprotection@nlcs.org.uk

26.2 If an individual believes the School has not complied with this policy or acted otherwise than in accordance with the UK GDPR, they should in the first instance notify the Data Protection Lead. The individual can also contact the ICO details of which can be found here: https://ico.org.uk/make-a-complaint/

27. Monitoring and review

27.1 The Headmistress, Senior Team and the Data Protection Lead will regularly monitor and evaluate the effectiveness of this policy, and associated procedures.

27.2 The policy will be reviewed every two years (or more frequently if changes to legislation, regulation or statutory guidance so require) by the Data Protection Lead and the relevant committee of the Governing Body.

27.3 The date of the next review is shown on the front page.

Appendix 1: CCTV footage access request form

The following information is required before the School can provide copies of or access to CCTV footage from which a person believes they may be identified.

Please note that CCTV footage may contain the information of others that needs to be protected.

Name and address: (proof of ID may be required)	
Description of footage (including a description of yourself, clothing, activity etc.)	
Location of camera	
Date of footage sought	
Approximate time (give a range if necessary)	

Signature* …….

Print Name …….

Date …….

*NB if requesting CCTV footage of a child under 13, a person with parental responsibility should sign this form. For children 13 or over, the child's authority or consent must be obtained except in circumstances where that would clearly be inappropriate and the lawful reasons to provide to the parent(s) outweigh the privacy considerations of the child.