Data Protection Policy

Ref: ***LP-MW-014***	Version: **2.2**	Date: *11th March 2021*
Document Owner: ***Angela Brassett (Finance Manager)***		
Description: This policy outlines the School's approach to managing personal data.		

OUR SCHOOL AIMS

- *To foster intellectual curiosity and a love of learning.*
- *To achieve high academic standards in a supportive but disciplined atmosphere.*
- *To equip pupils with the skills and knowledge to meet the challenges of our rapidly changing world.*
- *To instill an enthusiasm in interests and opportunities beyond the classroom.*
- *To support pupils' development of a sense of justice and an awareness of their rights and responsibilities as global citizens.*

1.0 POLICY STATEMENT AND PRINCIPLES

1.1 The Data Protection Act 1998 protects an individual's rights in the context of their information. Lingfield College and Lingfield College Prep process large amounts of personal data about members of the school community. Under the Data Protection Act, the school must process such personal data fairly. This includes telling pupils and parents how their personal data will be held and used by the school. This Data Protection Policy is intended to help meet that legal requirement. It should be noted 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.

1.2 This policy is intended 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. It 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. The General Data Protection Regulation (GDPR) is an EU Regulation which was to replace the current Directive and be directly applicable in all Member States without the need for implementing national legislation. It was adopted by the EU on 25 May 2018.

1.3 Anyone who works for, or acts on behalf of, the school (including staff, volunteers, Governors and service providers) should also be aware of and comply with this Data Protection Policy, which also provides further information about how personal data about those individuals will be used. Further details are in Section 3 and 4 of this policy.

1.4 The School is required to notify the Information Commissioner (ICO) of the processing of personal data. This information will be included in a public register which is available on the ICO website

1.5 In accordance with the Data Protection Act 1998, the school has notified the Information Commissioner's Office of its processing activities. The school's ICO registration number is Z4695808 and its registered address is Lingfield College, Racecourse Road, Lingfield, Surrey RH7 6PH

1.6 Lingfield College, as a corporate body, is named as the Data Controller for the school under the Act as it holds and uses personal information. The school decides how and why the information is used and has a responsibility to establish workplace practices and policies that are in line with the Act.

1.7 As Data Controller, Lingfield College must therefore:

- Manage and process personal data properly
- Protect the individual's right to privacy
- Provide an individual with access to all personal data held on them

1.8 The School has appointed the **Finance Manager** as **Data Protection Officer ("DPO")** who will endeavour to ensure that all personal data is processed in compliance with this policy and the Act.

1.9 'Personal data' relates to a living individual and allows that individual to be identified from it (either on its own or along with other information likely to come into the organisation's possession).

1.10 Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive.
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection

1.11 Lingfield College is committed to maintaining the principles at all times. This means that the school will:

- Inform the people whose data is being stored (so-called '**Data Subjects'**) why the school needs their personal information, how they will use it and with whom it may be shared. This is known as a '**Privacy Notice'**
- Check the quality and accuracy of the information held
- Apply the records management policies and procedures to ensure that information is not held longer than is necessary (either until a former pupil's 25th birthday, or longer in the case of Child Protection files)
- Reserve the right to keep data on Alumni where their permission has been received
- Ensure that when information is authorised for disposal it is done appropriately
- Ensure that appropriate security measures are in place to safeguard personal information whether it is held in paper files or on a computer system
- Only share personal information with others when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as '**Subject Access Request'** in the Data Protection Act 1998

- Train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures

2.0 TYPES OF DATA THAT ARE MANAGED BY THE SCHOOL

2.1 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
- Bank details and other financial information, e.g. about parents who pay fees to the school or payroll details for members of staff
- Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), examination scripts and marks
- Information about individuals' health, and contact details for their next of kin
- References given or received by the school about pupils and staff, and information (such as details on safeguarding concerns) provided by previous educational establishments and/or other professionals or organisations working with pupils
- Images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the school's CCTV policy on taking, storing and using images of children)

2.2 The school usually 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.

2.3 The school may, from time to time, need to process sensitive personal data regarding individuals. This type of data could include information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the school with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

2.4 As part of its operations, the school will use (and where appropriate share with third parties) personal data about individuals for a number of purposes, including:

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents
- To provide education services (including SEND support), careers advice and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni 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 or holiday clubs
- To monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's IT acceptable use 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
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school

3.0 DATA ACCURACY AND SECURITY

3.1 The school will endeavor 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 DPO of any changes to information held about them.

3.2 An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing.

3.3 The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, ensuring that it is held in accordance with the Principles of the Act. All staff will be made aware of this policy and their duties under the Act

4.0 SAFEGUARDING PRACTICE and INFORMATION SHARING

4.1 Whilst the Data Protection Act places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm.

4.2 Human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns. For further information, see HM Government's *"Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers"* (March 2015).

4.3 The Local Safeguarding Children Board (LSCB) can require an individual or body to comply with a request for information, as outlined in section 14B of the Children Act 2004. This can only take place when the information requested is for the purpose of enabling or assisting the LSCB to perform its functions. Any request for information about individuals should be necessary and proportionate to the reason for the request and should be made to Designated Safeguarding Leads or Safeguarding Coordinator who must discuss any such request with the Data Protection Officer.

5.0 RIGHTS OF ACCESS TO PERSONAL DATA ('SUBJECT ACCESS REQUEST')

5.1 Individuals have the right under the Act to access personal data about them held by the school, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO using the Subject Access Request form available on the website and from the DPO.

- Information about a child may be released to a person with parental responsibility, although the best interests of the child will also be taken into consideration. The child in question needs to be mature enough to understand their rights.
- Pupils aged 12 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case-by-case basis.

5.2 Parents should be aware that in certain situations they may not be consulted. 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.

5.3 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.

5.4 The ICO states that *'if the organisation is confident that the child can understand their rights, then it will respond to the child rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.' (ICO: Find out how to request your personal information')*

5.5 The school will endeavor to respond to any such written requests (known as "subject access requests") as soon as is reasonably practicable and in any event within the statutory time-limit of 30 calendar days from the date of receiving the Subject Access Request. According to the Information Commissioner's Office guidelines, the request may incur a charge.

5.6 If an individual believes that any information held on him or her is incorrect or incomplete, then they should write to the DPO as soon as possible. The School will promptly correct any information found to be incorrect

5.7 Information which an individual is entitled to access:

- Whether any data is being processed on the particular individual
- A description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- A copy of the personal data held
- Details about the source of the data

'Subject access provides a right for the requester to see their own personal data rather than a right to see copies of documents that contain their personal data. An organisation may choose to provide photocopies of original documents, but is not obliged to do so'. ***(ICO SAR Code of Practice Version 1.2 p8)***

5.8 Exemptions

- All members of the school community should be aware that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals, or information which is subject to legal professional privilege.

- The school is also not required to disclose any pupil examination scripts (though examiners' comments may, in certain circumstances, be disclosed), nor any reference given by the school for the purposes of the education, training or employment of any individual.

6.0 DATA PROTECTION FOR STAFF

The following Data Protection Code of Conduct should be adhered to at all times:

- Staff should only ever share information on a need to know basis
- Data protection should never be used as an excuse for not sharing information where necessary; the welfare of the child is paramount
- Seniority does not give an automatic right to information
- All emails are disclosable, less a few exemptions
- Only keep data for as long as is necessary (see Retention tables in Appendices A & B)

7.0 CONFIDENTIALITY

7.1 Any School information/records including details of pupils, parents and employees whether actual, potential or past, other than those contained in authorised and publicly available documents, must be kept confidential unless the School's prior written consent has been obtained. This requirement exists both during and after employment, and relates in particular to any information used for the benefit of any future employer.

7.2 The law states that where a teacher is facing an allegation of a criminal offence involving a pupil registered at the School, the teacher concerned is entitled to anonymity until the teacher is either charged with an offence or the anonymity is waived by the teacher. If publication is made on behalf of the School, the School, including Senior Management and Governors could be prosecuted.

7.3 If a teacher is charged with such an offence, all communication must be directed through the Headmaster who will have authority to deal with the allegation and any enquiries to ensure that this restriction is not breached. If a member of staff is found to have breached (whether intentionally or otherwise) this duty, any accusations will be dealt with under the School's Disciplinary Procedure.

8.0 OFF-SITE ACCESS TO PERSONAL DATA

8.1 The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data

8.2 The School is expected to ensure that measures are taken to avoid the accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the school community

8.3 ISAMS, the School's data management system, may be used on personal devices provided that the device is secure and password protected

8.4 For pupils on residential trips, medical information and other relevant information (e.g. passport details) may be taken off site by the trip leader but must be carefully managed and kept securely

9.0 USE OF PHOTOGRAPHS

The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

- Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken.
- Photos taken purely for personal use are exempt from the Act. However, please see the guidance given in the Lingfield College Staff Code of Conduct
- Photographs of pupils or students are taken for ISAMS. These images are stored electronically with other personal data and the terms of the Act will apply
- Photographs taken for the School website, prospectus or social media feeds are classed as personal data but will not breach the Act as long as the children and/or their parents are aware this is happening and the context in which the photo will be used
- Parental permission is sought through the Use of Photographs Form sent as part of the registration pack. Parents are given information about the types of uses made of the pupils' photographs, and are given the option to opt out. The names of pupils who are not allowed to feature in published photographs are made available to staff on the online Staff Handbook and are also displayed in the Staff Room and in the staff Photo Drive (S-Drive)

10.0 WHAT TO DO IN THE EVENT OF A SUSPECTED DATA BREACH

10.1 A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service" (*Data Breach Notification under the GDPR: Issues to Consider: Browne Jacobson LLP*)

10.2 A personal data breach may mean that someone other than the school gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within the school or if a member of staff accidentally alters or deletes personal data.

10.3 In the event of a breach, the member of staff must notify the Data Protection Officer within 24 hours of becoming aware of the breach. This notification must include at least:

- The member of staff's name and contact details
- The date and time of the breach (or an estimate)
- The date and time that the breach was detected it
- Basic information about the type of breach
- Basic information about the personal data concerned

10.4 The DPO will then make a judgement on the best course of action which is likely to include notifying the Headmaster, plus the Designated Safeguarding Lead in the event that the data breach includes pupils' details, as appropriate.

11.0 DATA PROTECTION FOR PUPILS AND FAMILIES

11.1 The school will use the contact details of parents, alumni 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 by post.

11.2 With permission from the relevant individual, the school may also:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the school community, such as the Lingfield Parents' Association (LPA)
- Contact parents and/or alumni by post and email in order to promote and raise funds for the school

11.3 If any member of the school community wishes to limit or object to any such use, or would like further information about them, they should contact the DPO in writing

11.4 Pupils are required to respect the personal data and privacy of others, and to comply with the school's IT Acceptable Use Policy and the school rules (Pupil Code of Conduct)

12.0 QUERIES AND COMPLAINTS

12.1 Any comments or queries on this policy should be directed to the DPO using the following contact details: Angela Brassett, Data Protection Officer, Lingfield College, St Pier's Lane, Lingfield, Surrey RH7 6PN

12.2 If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the school complaints procedure and should also notify the DPO

13.0 DATA RETENTION AND STORAGE GUIDELINES

13.1 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 Act, but not all.

13.2 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.

14.0 PUPIL RECORDS:

14.1 Guidance on maintaining pupil records can be found in the *IRMS Information Management Toolkit for Schools 2016* and the following information is kept by Lingfield College and Lingfield College Prep School.

14.2 These guidelines apply to information created and stored in both physical and electronic format. The pupil record starts its life when a file is opened for each new pupil as they begin school. This is the file which will follow the pupil for the rest of his/her school career.

14.3 If pre-printed file covers are not being used then the following information should appear on the front of the paper file:

- Surname
- Forename
- DOB

14.4 Inside the pupil's folder the following information should be easily accessible:

- The name of the pupil's doctor
- Emergency contact details
- Gender
- Preferred name
- Position in family
- Ethnic origin
- Language spoken at home (if other than English)
- Religion
- Any allergies or other medical conditions that it is important to be aware of
- Names of adults who hold parental responsibility with home address and telephone
- Number (and any additional relevant carers and their relationship to the child)
- Name of the school, date of admission
- Date of leaving
- Any other agency involvement e.g. speech and language therapist, paediatrician

14.5 Items which should be included in the pupil record:

- If the pupil has attended an early years setting, then the record of transfer should be included on the pupil file
- Admission form (application form)
- Most recent Privacy Notice
- Photography Consents
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in a sealed envelope clearly marked as such or in a separate medical file)
- Child protection reports/disclosures (should be stored in a separate file with a sticker on the front to indicate that there is another CP file on that child)

- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

14.6 The following records are subject to shorter retention periods and do not need to be transferred to the pupil's next school:

- Absence notes
- Parental consent forms for trips/outings (in the event of a major incident the parental consent forms should be retained with the incident report not in the pupil record)
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)

15.0 TRANSFERRING THE PUPIL RECORD TO ANOTHER SCHOOL (LINGFIELD COLLEGE OR ELSEWHERE)

15.1 The pupil record should not be weeded before transfer to the secondary school unless any records with a short retention period have been placed in the file. It is important to remember that the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage.

15.2 The Prep School does not need to keep copies of any records in the pupil record except if there is an ongoing legal action when the pupil leaves the school. Custody of and responsibility for the records passes to the school the pupil transfers to.

15.3 Files should not be sent by post unless absolutely necessary. If this does need to happen, then files should be sent by registered post with an accompanying list of the files included in the parcel. The new school should sign the enclosed form to say that they have received the files and return the form to Lingfield College or Lingfield College Prep School. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes.

15.4 Electronic documents (including Safeguarding information, where relevant) that relate to the pupil file also need to be transferred, or, if duplicated in a master paper file, destroyed.

16.0 STORAGE OF RECORDS

16.1 All pupil records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security. Access arrangements for pupil records should ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

16.2 In order to mitigate against the loss of electronic information, the school operates a back-up system for all information held electronically to enable the restoration of the data in the event of an environmental or data corruption incident.

16.3 Digital Records

- Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive 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
- **Personal information should not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff are advised not to hold personal information about students or other staff on mobile storage devices including memory sticks, phones, tablets, portable hard drives or even on CDs**
- The School asks students and staff to change their passwords on a termly basis. Password sharing is strongly discouraged and alternative ways of sharing data are used such as shared Google Drive
- Emails, whether they are retained electronically or printed out as part of a paper file are also "records" and may be particularly important: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record
- It is important that all staff bear in mind, when creating documents and records of any sort (and particularly email), that at some point in the future those documents and records could be disclosed - whether as a result of litigation or investigation, or because of a Subject Access Request under the Act. It is therefore crucial that all documents are accurate, professional and as objective as possible

16.4 Paper records

- Under the Act, paper records are only classed as personal data if held in a "relevant filing system" – i.e. one that is organised, and/or indexed, so that specific categories of personal information relating to a certain individual are readily accessible, and thus searchable as a digital database might be. An example of this could be an alphabetical personnel file split into marked dividers which would fall under this category, but a merely chronological file of correspondence may well not.
- However, when personal information is contained on print-outs taken from electronic files, this data has already been processed by the school and falls under the Act.

16.5 Any live lessons could be recorded and backed up. As these recordings contain personal images of identifiable people, they must be kept secure.

Any lessons that are recorded are done so to investigate any complaints that might arise, or for crime prevention and investigation. Recordings will be kept as per the recommended retention periods in Appendix A

17.0 THE ARCHIVING AND ERASURE OF RECORDS

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

- Records - whether electronic or hard copy – should be stored securely, encrypted if possible, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable

- Important records, and large or sensitive personal databases should not be taken home or - in the case of digital data - carried or kept on portable devices (whether memory sticks, mobile phones or other electronic equipment) unless absolutely necessary
- Issues of back-up or migration are approached in line with general school policy (such as professional storage solutions or IT systems) and not individual ad hoc action
- Arrangements with external storage providers - whether physical or electronic (in any form, but particularly "cloud-based" storage) – must be supported by robust contractual arrangements providing for security and access
- Reviews must be conducted on a regular basis in line with the guidance on suggested retention periods, to ensure that all information being kept is still relevant and (in the case of personal data) necessary for the purposes for which it is held
- The destruction or permanent erasure of records, if undertaken by a third party, must be carried out securely - with no risk of the re-use, disclosure or re-construction of any records or the information contained in them
- 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
- Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / discs should be cut into pieces. Hard-copy images, AV recordings and hard drives should be dismantled and destroyed and old PCs must be wiped clean
- Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information securely

18.0 COVID TESTING IN SCHOOL

18.1 In line with government requirements the School has set up and implemented COVID testing on site for staff and senior school pupils, and at home for Prep School staff. The School is responsible for the processing of the test.

18.2 All participants who are tested have to give prior medical consent for either themselves (staff) or their child (parent) to take the test. Such consent also gives agreement to the processing of associated personal data.

18.3 The lawful basis for the processing of the test and the personal data is Public Task where it is necessary to process personal data to ensure the School meets its obligations in education legislation to safeguard and promote the wellbeing of pupils. Public Health legislation also allows the sharing of personal data with Department of Health and Social Care (DHSC), local government, Test and Trace and the NHS.

18.4 The personal data collected is requested by the government application when registering for a test and being assigned a unique barcode. The government application will also record the results, and advise staff and/or parents of any positive result.

18.5 All testing is voluntary and anyone who refuses a test will have that decision recorded so they are not persistently asked to agree to a test.

18.6 The School will not tell any unauthorised person (that is anyone not involved in the recording of test results) of any tests taken, test refusals or positive/negative test results.

19.0 RELATED POLICIES

- Admissions
- Attendance and Registers
- Behaviour Management
- CCTV
- Complaints
- Computer Usage
- Disability
- Educational Visits
- Equal Opportunity and Racial Equality
- E-Safety
- Exclusion
- First Aid
- Health & Safety
- Mental Health (including Eating Disorders and Self-harm)
- Risk Assessment
- Safe Staff Recruitment
- Safeguarding & Child Protection
- SEND Policy (including the Accessibility Plan)
- Staff Code of Conduct
- Whistleblowing

Policy created March 2021

Next review due March 2022

APPENDIX A

Recommended Retention Periods

Category of Data	Type of Document	Suggested Retention Period*	Responsibility
School-specific Records	The School's registration documents	**Permanent**	Admissions
	Daily Attendance Register	**6 years**	Data Manager (ISAMS)
	Minutes of Governors' Meetings	**Permanent**	Clerk to the Governors
	Annual Curriculum Material	**3 years** from the end of the relevant academic year **3 years** for other class records – marks, timetables, assignments	Teaching Staff
Individual Pupil Records	Admissions: Application forms, entrance examinations, records of decisions	Up to **7 years** from pupil leaving school (if admitted) Up to **7 years** from decision to reject	Admissions
	Examination results (internal and external)	**7 years** from the pupil leaving school; Prep School test papers are destroyed on leaving, other than Year 6 examinations	Teaching Staff Data Manager Examinations Officer Prep School Archivist
	Pupil File (including reports); An extra sticker on this file signifies that the child also has a Child Protection File	**25 years** from date of birth	DSL Office Staff
	Child Protection Files	**25 years** from date of birth, after which the case is reviewed	DSL
	Pupil Medical Records	**25 years** from date of birth	Office Staff

	Pupil Performance Records	**7 years** from the pupil leaving school (unless there is good reason to reason to consider they may be applicable evidence in a medical, negligence or abuse claim)	Data Manager Prep School Archivist
	SEND Records (to be assessed individually)	Up to **35 years** from the pupil's date of birth (allowing for special extensions to statutory limitation period)	SENDCo
Specific Events	Information such as guest lists, personal contact details, financial information and dietary requirements	For no longer than is necessary to conduct the event; to provide information for future events	Event Organiser
Safeguarding	Policies and procedures	Permanent record of historic policies	DSL
	DBS disclosure certificates	No longer than 6 months from decision on recruitment unless DBS specifically consulted Employee keeps their own copy Keep record that checks were made, even if not the information itself Potentially sensitive personal data must be kept secure	HR
	Reporting of Incidents	Where an issue or concern relating to a member of staff and the safeguarding of children has been identified, records of any concerns, suspicions or investigations will be kept for **75 years** by the DSL Allegations which prove to be malicious will not be kept as part of the personnel record.	DSL HR

		Limitation periods can be disapplied in criminal and civil abuse cases; to be weighed against rights under the DPA and insurers' requirements.	
Digital Images	Photographs of students involved in school activities	Until the child reaches their 25th birthday, or for longer with specific written consent from Alumni	Marketing Manager Teaching Staff Prep School Archivist
Digital recordings	Digital recording of live lessons	**6 months**	Deputy Head Academic
Corporate Records	Certificates of Incorporation	**Permanent**	Finance
	Minutes, notes and resolutions of Boards or Management meetings	**Permanent**	Finance
	Register of Members and Shareholders	**Permanent**	Finance
	Annual Reports	Minimum **6 years**	Finance
Accounting Records**	Accounting Records (ie records which give an accurate picture of a company's financial position & which give a true and fair view of the company's financial state)	Minimum **6 years** for UK charities (and public companies) from the end of the financial year in which the transaction took place.	Finance
	Tax Returns	Minimum **7 years**	Finance
	VAT Returns	Minimum **7 years**	Finance
	Budget & Internal Financial reports	Minimum **6 years**	Finance
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	Finance
	Deeds (or contracts under seal)	**Permanent**	Finance
Intellectual Property Records	Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks);	Finance

		otherwise **expiry of right** plus minimum of **7 years**	
	Assignments of intellectual property to or from the school	**7 years** minimum (contracts); where applicable, **13 years** (deeds)	Finance
	IP/IT Agreements (including software licences and ancillary agreements eg maintenance; storage; development; co-existence agreements; consents)	Minimum **7 years** from completion of contractual obligation concerned or term of agreement	Head of Estates & Facilities
Insurance Records	Insurance certificates (private, public, professional indemnity)	**Permanent**	Finance
	Correspondence related to claims / renewals / notification re insurance	**Permanent**	Finance
Pension Records	Pension records for pension funds managed by the school for support staff	**Permanent**	Finance
Environmental & Health Records	Maintenance logs	**10 years** from date of last entry	Head of Estates & Facilities
	Accidents to Children***	**25 years** from date of birth	Head of Estates & Facilities H&S
	Accident at work records (Staff)***	Minimum **4 years** from date of accident, but review case-by-case where possible	Head of Estates & Facilities H&S
	Staff use of hazardous substances****	Minimum **7 years** from end of date of use	Head of Estates & Facilities H&S
	Risk Assessments*** (carried out in respect of above)	**7 years** from completion of relevant project, incident, event or activity	Head of Estates & Facilities H&S

* Basis of suggestion: Some of these will be mandatory legal requirements (eg under the Companies Act 2006 or the Charities Act 2011). Any suggestions where there are no legal mandatory requirements are based on advice from the Independent

Schools Bursars' Association (ISBA). Practical considerations for retention such as limitation periods for legal claims, weighed against whether there is a reasonable argument in respect of data protection.

** Retention period for tax purposes should always be made by reference to specific legal or accountancy advice.

*** 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, and keep a record that they were followed.

APPENDIX B

Standard Recommended Employment Records: Retention Periods

Type of Employment Record	Statutory or Code of Practice Reference	Format & Location	Retention Period
Job applications and interview records of unsuccessful candidates	The ICO Employment Practices Code	Paper/electronic	**6 months** after notifying unsuccessful candidates.
Personnel and training records	N/A	Paper/electronic	While employment continues and up to **6 years** after employment ceases
Written particulars of employment; contracts of employment; changes to terms & conditions	N/A	Paper/electronic	While employment continues and up to **6 years** after employment ceases
Working time opt-out forms	Working Time Regulations (WTR)	Paper/electronic originals are not required by the WTR	**2 years** from the date on which they were entered into
Records to show compliance with the Working Time Regulations (WTR)	Working Time Regulations (WTR)	Paper/electronic	**2 years** after the relevant period
Annual Leave Records	N/A	Paper/electronic	**6 years**
Payroll & wage records for companies	Finance Act 1988	Paper/electronic	**7 years** from the financial year end in which payments were made
PAYE (Pay as you Earn)	Income Tax Regulations 2003	Paper/electronic	**7 years** from the financial year end in

			which payments were made
Maternity Records	Statutory Maternity Pay Regulations 1986	Paper/electronic	**7 years** from the financial year end in which payments were made
Sickness Records required for the purposes of Statutory Sick Pay (SSP)	Statutory Sick Pay Regulations 1982	Paper/electronic	**7 years** from the financial year end in which payments were made
Current bank details	N/A	Paper/electronic	No longer than necessary
Records of advances of loans to employees (now ceased)	N/A	Paper/electronic	While employment continues and up to **6 years** after repayment
Death Benefit Nomination and Revocation Forms (from September 2018)	N/A	Paper/electronic	**Permanent** during staff member's employment