Windlesham School & Nursery

Data Protection Policy

Reviewed: September 2023

Next Review Due: September 2025

Reviewed by John Ingrassia, School Consultant

In accordance with the UK Data Protection Act 2018 the School has notified the Information Commissioner's Office (ICO) of its processing activities. The school's ICO registration number is Z3004010. Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register. Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

It will be made clear to parents in the admissions documentation that by accepting a place at the school, they agree to the school's data protection policy. They will be directed to the school portal where a copy of the policy is available so that they are aware about how their personal data will be used.

About this Policy

Everyone has rights regarding the way in which their personal data is handled. During the School's activities it collects, stores and processes personal data about staff, pupils, their parents, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

This policy sets out the basis on which the School will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time. This policy should be read alongside the Windlesham School Privacy Notice 2022.

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements. The legal basis for processing data is that it is necessary to carry out these tasks in the public interest.

The member of staff directly responsible for data protection is the School Bursar, also known as the Data Protection Controller (DPC). They will work in partnership with JSPC, our technical service providers, the governors, headteacher and the Senior Leadership Team. Indirectly, all Windlesham School staff will be involved in ensuring compliance with the policy.

The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

General Statement of the School's Duties

The School is required to process relevant personal data regarding workers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Aims & Objectives

The aim of this policy is to provide a model set of guidelines to enable staff, parents and pupils to understand:

The law regarding personal data

How personal data should be processed, stored, archived and deleted/destroyed

How staff, parents and pupils can access personal data.

The objective of the policy is to ensure that the School acts within the requirements of the UK Data Protection Act (DPA) 2018 when retaining and storing personal data, and when making it available to individuals, and that the process of responding to enquiries for other information is also legal under the Freedom of Information Act 2000 (in force from 1st January 2005).

The Principles

- Anyone processing personal data must comply with the eight enforceable principles of good practice as enshrined within the Data Protection Act 1998. These provide that personal data must be:
- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Data Protection – the law

- Under the DPA (2018), and other regulating acts, access to their own personal information is a statutory right for pupils (if they are of an age to understand the information they request) and parents (as defined in the Education Act 1996) may also request access to their child's personal data.
- School staff have a right of access to personal data on themselves.
- Anyone has the right to question and correct inaccurate information, but this must address matters of fact, not opinion.
- Personal data should always be kept securely and protected by passwords if it is electronic. Access to data should only be by those authorised to see it. Confidentiality must be respected at all times.
- Personal data should not be kept longer than is required.
- Third party data (information about someone other than the requesting individual) should in general only be provided with their permission.
- Personal data should always be of direct relevance to the person requesting the information. A document discussing more general concerns may not be defined as personal data.

Responsibility for Data Protection

The School has appointed Samantha Roberts as the Data Protection Controller (DPC) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Controller.

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: What is personal information: a guide

Personal Data

Personal data covers information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, pupils and their parents, suppliers and marketing and business contacts. It includes expressions of opinion about the individual, any indication of someone else's intentions towards the individual, information necessary for employment such as the worker's name and address and details for payment of salary.

It includes all information in education records, including names, dates of birth, addresses, school marks, medical information, exam results, and SEN assessments.

Sensitive Personal Data

The School may from time to time, be required to process sensitive personal data regarding a worker. Where sensitive personal data is processed by the School, the explicit consent of the worker will generally be required in writing.

The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the DPC for more information on obtaining consent to process sensitive personal data.

Information relating to race and ethnicity, political opinions, religious beliefs, physical or mental health, sexuality and criminal offences is "sensitive" personal data and particular care must be taken in storing and processing such data.

Guidance on accuracy, adequacy, relevance and proportionality

Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask the School to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the DPC.

Staff must ensure that personal data held by the School relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the DPC so the School's records can be updated.

Accuracy

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

Fair Processing of Personal Data and Data which may be shared

The School's policy is to process personal data in accordance with the applicable data protection laws. All staff have a personal responsibility for the practical application of this policy.

Staff should generally not process personal data unless:

- The individual whose details are being processed has consented to this
- The processing is necessary to perform the Schools legal obligations or exercise legal rights
- The processing is otherwise in the Schools legitimate interests and does not unduly prejudice the individual's privacy.

When gathering personal data, or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. There are limited exceptions to this notice requirement as noted below. In any case of uncertainty as to whether a notification should be given, staff should contact the DPC.

- Personal data and school records about pupils are confidential to the child. The information can be shared appropriately within the professional working of the school to enable the school to make the best educational provision for the child. The law permits such information to be shared with other educational establishments when pupils change schools.
- School records for a child should be kept for 7 years after the child leaves the school, or until the child reaches 25 years of age (whichever is greater) and examination records the same. (See Appendix A)
- Data on staff is sensitive information and confidential to the individual, and is shared, where appropriate, at the discretion of the Head Teacher and with the knowledge and, if possible, the agreement of the staff member concerned.
- Employment records form part of a staff member's permanent record. Because there are specific legislative issues connected with these (salary and pension details etc.) these records should be retained. (See Appendix A)
- Interview records, CV's and application forms for unsuccessful applicants are kept for 6 months. (See Appendix A)
- All formal complaints made to the Head Teacher or School Governors will be kept for at least seven years in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and to legal professional privilege in the event of a court case. (See Appendix A)

Guidance on accessing personal data

- Parents should note that all rights under the DPA (2018) to do with information about their child rest with the child as soon as they are old enough to understand these rights. This will vary from one child to another, but, as a broad guide, it is assumed that most children will have a sufficient understanding by the age of 12. Parents are encouraged to discuss and explain any request for information with their child if they are aged 12 or over.
- A parent can request access a copy of their child's school records and other information held about their child. The request must be made in writing. There is no charge for such requests on behalf of the child, but there may be a charge for photocopying records – this is detailed in guidance available from the Information Commissioner. Staff should check, if a request for information is made by a parent, that no other legal obstruction (for example, a court order limiting an individual's exercise of parental responsibility) is in force.
- For educational records, unlike other personal data, access must be provided within 15 school days, and if copies are requested, these must be supplied within 15 school days of payment. Details of allowable charges can be found on the Information Commissioners website (www.ico.gov.uk).
- A member of staff can request access to their own records at no charge, but the request must be made in writing. The member of staff has the right to see their own records, and to ask for copies of the records. There is no charge for copies of records.
- The law requires that all requests for personal information are dealt with within 40 days of receipt except requests for educational records (see above). All requests will be acknowledged in writing on receipt, and access to records will be arranged as soon as possible. If awaiting third party consents, the School will arrange access to those documents already available, and notify the individual that other documents may be made available later.
- In all cases, should third party information (information about another individual) be included in the information staff will try to obtain permission to show this information to the applicant, with the exception of information provided by another member of school staff (or local authority staff) which is exempt from a requirement for third party consents. If third party permission is not obtained the person with overall responsibility should consider whether the information can still be released.
- A request for personal information can include unstructured as well as structured records – for example, letters, emails etc. not kept within an individual's personal files, or filed by their name, but still directly relevant to them. If these would form part of a wider record it is advisable to file these within structured records as a matter of course and to avoid excessive administrative work. These can be requested if sufficient information is provided to identify them.
- Anyone who requests to see their personal data has the right to question the accuracy of matters of fact within the data, and to ask to have inaccurate information deleted or changed. They may also question opinions, and their comments will be recorded, but opinions do not need to be deleted or changed as a part of this process.
- The school will document all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes (letter requesting changes etc.) This will enable staff to deal with a complaint if one is made in relation to the request.
- Some School data is held digitally and this should be password protected. (See eSafety Policy for further information about electronic data storage.)

Timely Processing

The School will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required.

Appendix A lists suggested retention periods for a range of data.

Rights of Individuals

Individuals have the right of access to information held by the School about them, subject to the provisions of the DPA (2018). Any member of staff, parent, visitor, contractor, governor etc wishing to access their personal data should put their request in writing to the DPC. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, according to the guidance from the ICO https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-of-access/

The School may charge for the provision of the requested personal data, as permitted by law and using the ICO guidelines. The information will be imparted to the individual as soon as is reasonably possible after it has come to the School's attention. It should be noted that there are certain restrictions on the information to which individuals are entitled under applicable law.

Staff should not send direct marketing material to someone electronically (e.g. by email) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their personal data for direct marketing purposes and should notify the DPC about any such request. Staff should contact the DPC for advice on direct marketing before starting any new direct marketing activity.

Exemptions

Certain data is exempted from the provisions of the Data Protection Act. This includes the following:

- The prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

Any further information on exemptions should be sought from the DPC.

Enforcement

If a staff member believes that the School has not complied with this Policy or acted otherwise than in accordance with the DPA, the staff member should utilise the School grievance procedure also notifying the DPC.

Data Security

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO: A Guide to Data Protection Principles

Security measures will be applied in relation to data belonging to both staff and pupils. As such, no member of staff is permitted to remove personal data from School premises, whether in paper or

electronic form and wherever stored, without prior consent of the Headteacher or Bursar. Where a worker is permitted to take data offsite it will need to be encrypted. (See Online Safety Policy.)

Archiving and the destruction or erasure of Records

All Staff will receive basic training biennially by the DPC in data management including issues such as security, recognising and handling sensitive personal data, safeguarding etc. This will also form part of their induction on starting with the school.

Staff given specific responsibility for the management of records will have specific training and ensure, as a minimum, the following:

- Records - whether electronic or hard copy - are stored securely, 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, will not be taken home or - in respect of digital data - carried or kept on portable devices (whether CDs or data sticks, or mobiles and handheld electronic tablets) unless absolutely necessary. If it is necessary, a risk assessment will be carried out. For further details refer to the School eSafety Policy.
- Information is backed-up and transferred as recommended by our Technical Service Providers and not individual *ad hoc* action.
- Arrangements with external storage providers - whether physical or electronic (in any form, but most particularly "cloud-based" storage) - are supported by robust contractual arrangements providing for security and access.
- Reviews of data processing procedures are conducted on a regular basis, in line with the review of this policy, 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 (and if so, that it is accurate and up-to-date).
- 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 re-construction, of any records or information contained in them.

Location of information and data:

Hard copy data including registration records, medical records and personal academic records are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day such as an Emergency Care Plan. This will be displayed in the Staffroom and will include only the absolutely necessary information for the execution of a medical intervention.

Sensitive or personal information and data in hard copy form should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

Secure disposal of documents

- Confidential, sensitive or personal information is disposed on site or via a confidential waste disposal expert to ensure that it cannot be read or reconstructed.
- Paper records are shredded using a cross-cutting shredder; CDs / DVDs are 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 under adequate contractual obligations to the school to process and dispose of the information securely.

Review

This policy will be reviewed and updated every two years.

Additional Information

Information Commissioner's Code of Practice Guidelines (ICC of P Guidelines) are available on the internet www.ico.gov.uk

APPENDIX A

Storage and retention of documents/information

TABLE OF SUGGESTED RETENTION PERIODS

(Guidance from Independent Schools' Bursars Association at February 2016. Except where there is a specific statutory obligation to destroy records, guidance does not constitute prescriptive time 'limits'. Thought and judgement will need to be exercised or advice taken depending on different circumstances. Some of these periods will be mandatory legal requirements (e.g. under the Companies Act 2006 or the Charities Act 2011), but in most 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.)

Type of Record/Document	**Suggested Retention Period**
SCHOOL-SPECIFIC RECORDS • Registration documents of School • Attendance Register • Minutes of Governors' meetings • Annual curriculum	• Permanent (or until closure of the school) • 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: e.g. marks / timetables / assignments

INDIVIDUAL PUPIL RECORDS
• Admissions: application forms, assessments, records of decisions
• Examination results (external or internal)
• Pupil file including:
  ○ Pupil reports
  ○ Pupil performance records
  ○ Pupil medical records
• Special educational needs records (to be risk assessed individually)
	NB - this will generally be personal data
	• 25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
	• 7 years from pupil leaving school
	• 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 pupil.
	• Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)

SAFEGUARDING • Policies and procedures • DBS disclosure certificates (if held) • Incident reporting	• Keep a permanent record of historic policies • No longer than 1 month from decision on recruitment, unless DBS specifically consulted - but a record of the checks being made must be kept, if not the certificate itself. • 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. (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.)
CORPORATE RECORDS • Certificates of Incorporation	• Permanent
• Minutes, Notes and Resolutions of Boards or Management Meetings	• Minimum - 10 years
• Shareholder resolutions	• Minimum - 10 years
• Register of Members/Shareholders	• Permanent (minimum 10 years for ex-members/shareholders)
• Annual reports	• Minimum - 6 years
ACCOUNTING RECORDS (*Retention period for tax purposes should <u>always</u> be made by reference to specific legal or accountancy advice).* • Accounting records *(normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*) [NB <u>specific ambit to be advised by an accountancy expert</u>]	• Minimum - 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place
• 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*)	• Minimum - 7 years from completion of contractual obligations or term of agreement, whichever is the later
• Deeds (or contracts under seal)	• Minimum - 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS • Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	• Permanent (in the case of any right which can be permanently extended, 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; co-existence agreements; consents)	• Minimum - 7 years from completion of contractual obligation concerned or term of agreement

EMPLOYEE / PERSONNEL RECORDS • Single Central Record of employees • Contracts of employment	**NB this will almost certainly be personal data** • Keep a permanent record of all mandatory checks that have been undertaken • 7 years from effective date of end of contract
• Employee appraisals or reviews • Staff personnel file	• Duration of employment plus minimum of 7 years • 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 RECORDS *(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.)* • Maintenance logs • Accidents to children	• 10 years from date of last entry • 25 years from birth (unless safeguarding incident)
• Accident at work records (staff)	• Minimum - 4 years from date of accident, but review case-by-case where possible
• Staff use of hazardous substances • Risk assessments (carried out in respect of above)	• Minimum - 7 years from end of date of use • 7 years from completion of relevant project, incident, event or activity.