Wakefield Grammar School Foundation

Document Reference	**WGSF Data Retention Storage & Disposal Policy**
Version Number	V1.03
Author/Lead **Job Title**	Vicky Weeks, Compliance Manager
Checker Person Name **Quality Assurance**	Jenny Cocker, Director of Finance and Operations
Consultation	Director of Finance and Operations
Name of Ratifying Committee **Date Ratified**	Risk, Compliance and Governance Committee 05.11.2024
Date of Next Review (Annually)	**November 2025**

VALIDITY – Policies should be accessed via FireFly to ensure the current version is used.

CHANGE RECORD - REVIEW PERIOD (Annually)

Version	Date	Change details
V1.01	Jan 2021	Reviewed (Sally Williams-McGlone)
V1.02	June 2023 Sept 2023	Reviewed and updated with processes for staff Vicky Weeks Reviewed, V Weeks
V1.03	Oct 2024	Updated in line with ISBA guidance, V Weeks

To be published on the following:

Staff shared	**X**	**School website**	**X**

WGSF Data Retention Storage & Disposal Policy

1. Introduction

Wakefield Grammar School Foundation (WGSF), referred to as 'the Foundation', incorporates Queen Elizabeth Grammar School (QEGS), Wakefield Girls' High School (WGHS) and Wakefield Grammar Pre-Prep School, delivering education to children aged 3 - 18.

Data protection is an important legal compliance issue for the Foundation. This policy details the expected behaviours of the Foundation's employees and third parties in relation to the storage, retention and disposal of any personal data record belonging pupils, parents, employees and other data subjects. It should be read in conjunction with other Foundation Policies including:

- WGSF Privacy Notices
- WGSF Data Protection Policy
- WGSF CCTV Policy
- WGSF ICT Acceptable Use Policy

Please note this is not an archiving guide / policy, which is the subject of separate guidance.

2. Meaning of 'Record'

In this policy, "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, but not all, will contain personal data of individuals as defined in GDPR.

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 for retention purposes than its contents, and the reason for keeping it.

Digital Records

All electronic records must be stored securely, including if possible with encryption. Important records and large or sensitive personal databases must not be taken home or kept on unencrypted portable devices.

Arrangements with external storage providers, whether physical or electronic (most particularly "cloud-based" storage) must be supported by robust contractual arrangements providing for security and access.

Please refer to the WGSF ICT Acceptable Use policy for further information.

Email accounts and internal messaging systems

Emails and other internal messages – whether they are retained electronically or printed out as part of a paper file – are also "records" likely to contain personal data (of the sender, recipient, or a third party) in their body, footer, in the sent/received fields, or in attachments. As such they will potentially fall within the scope of a subject access request made against the school.

The Foundation recommends its staff to have an email retention of no more than 2 or 3 years (see Appendix 1). Following this recommendation ensures that staff are not relying on email accounts to retain important information, resources, contracts, legal advice, attendance

notes, safeguarding concerns or incident reports that ought to be properly held in the appropriate file, accessed only by the appropriate persons.

Records on personal devices including SMS / WhatsApp

As a general rule, an employee has an expectation of privacy in their own messaging for personal use, and is not subject to UK GDPR for solely domestic or 'household' uses of data. However, where personal devices are used by employees or governors for official school use – for example to discuss a pupil issue, parental complaint or disciplinary matter – **it may be deemed an official record** of the school. This means it may be disclosable in litigation or under a subject access request, if the school has reasonable grounds to believe relevant evidence or personal data might be found on the device, including by SMS, WhatsApp or personal email. In that sense, any staff or governor WhatsApp group must be used with the same professional formality as email.

Paper records

Paper records can be damaged by damp or poor storage conditions and therefore need to be stored in dry, cool, reasonable ventilated areas. Security is also vital, especially if the materials contain legally or financially sensitive data, as well as data personal to individuals.

Under GDPR, paper records are only classed as personal data if held in a qualifying "filing system". This means organised, and/or indexed data which is readily accessible, e.g. personnel files searchable by marked dividers will likely fall under GDPR. A daily notebook, or diary, or chronological file of correspondence may not, unless it is readily clear to whom the file or notebook substantially relates to.

Staff within the Foundation should not retain or store personal data in disorganised or inaccessible hard copies (except as part of an appropriate archiving policy which may be subject to an exemption from data protection rules) as the Foundation remains responsible for data security including personal information contained on handwritten notes, print-outs taken from electronic files, or disclosures from systems made orally.

3. When it is lawful to retain 'personal data'

Most records contain information about living individuals: e.g. pupils, parents, alumni, governors, staff (past, present and prospective), and consultants / contractors etc. Others contain information on professional contacts. These types of information are likely to amount to "personal data" and therefore be subject to data protection laws which link with 'document retention'.

Generally, the sources of law that determine how long we should retain personal data for e.g. statutory time limits by which legal claims must be made; the stipulations of our contracts; or the requirements of governmental organisations (e.g. the Disclosure and Barring Service, Charity Commission etc.)

Data protection law requires that personal data is only retained for as long as necessary and only as much as is necessary for the specific lawful purpose(s) it was acquired, or at least for clearly compatible purposes. Most "ordinary" personal data may be processed in connection with a private contractual duty (e.g. under an employment or parent contract) or where necessary for a "legitimate interest" as defined in GDPR (please refer to our Privacy Notices for further information on this). It may then be retained for a reasonable and necessary period of time generally linked to legal claims.

A higher standard would apply to the processing of "special category personal data", including health, trade union membership, ethnicity, religious beliefs, political views and sexual life. Similar rules also apply to any records of criminal proceedings, offences or allegations. As this may be required in connection with the defence of future legal claims, or to help prevent or detect crime or unlawful behaviour, or as part of the school's safeguarding duties, the retention period is longer.

Please refer to the Data Retention table guide in Appendix 1 for the Foundation's recommended retention period.

4. The risks of longer retention

The longer personal data is retained, and the more sensitive material is kept on file, the greater the administrative and storage burden is on the Foundation. This also increases the amount of material in respect of which the Foundation must be accountable to data subjects (e.g. information requests, "right to be forgotten" requests etc.), and the consequences of data security breach become more serious.

It is also vitally important that all staff bear in mind that when creating documents and records of any sort, 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 GDPR. **Record-keeping must therefore be accruate, clear and professional.**

6. Secure disposal of documents and devices

Saff are asked to consider one of two actions at the end of a document's "life": secure deletion, or archiving.

For confidential, sensitive or personal information to be securely disposed of it must be in a condition where it cannot either be read or reconstructed:

- for hard copy documents, skips and 'regular' waste disposal will not be considered secure;
- Paper records or images should be shredded using a cross-cutting shredder;
- devices for digital storage and recordings should be dismantled or broken into pieces.

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.

The Foundation's Digital Services will arrange the safe destruction/wiping of digital devices. This may include a number steps prior to disposal, including:

- wiping the hard drive and/or activating drive encryption;
- uninstalling and/or deauthorising applications or accounts that could enable a user to access secure school systems (including wiping browsing history and cookies); and/or:
- physically destroying the drive.

Staff should retain a log of the type of data, when it is disposed of, how it is disposed of and who disposed of it for future reference. **See Appendix 2.**

Appendix 1: Data Retention Guide

The figures suggested in the table are, in most cases, guides as to what are periods of reasonable necessity that could be defensible if challenged.

Some of these periods will be mandatory legal requirements (e.g. under the Companies Act 2006 or the Charities Act 2011, as applicable), but in the majority of cases these decisions are what the Foundation have agreed as reasonable 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**
Emails on Server	Pupil email account	Delete upon leaving school, or within one year
	Staff emails	Routine deletion of historic emails after 2-3 years Delete account within 1 year of leaving school.
School Specific Records	Registration documents of school	Permanent (or until closure of the school)
	Attendance Register	6 years from the last date of entry, then archive
	Minutes of governor meetings	6 years from date of meeting
	Annual curriculum	From end of year: 3 years (or 1 year for other class records: e,g, marks / timetables / assignments)
Complaints	Documentation and records pertaining to complaints	Minimum of 7 years unless they concern allegations of abuse where they should be preserved for the term of the Independent inquiry into Child Sexual Abuse and at least until the accused has reached normal pension age or for 10 years from the date of the allegation if it is longer.
Individual Pupil Records *NB these will contain personal data*	Admissions: application forms, assessments, records of decisions	25 years from date of birth (or up to 7 years from the pupil leaving). If unsuccessful: up to 1 year
	Student immigration records	Duration of student sponsorship plus min. 1 year
	Examination results (external or internal)	7 years from pupil leaving school
	Pupil file including: - Pupil reports and performance records - Pupil medical records (not accidents)	ALL: 25 years from date of birth *(subject where relevant to any material that may be relevant to potential historic claims: see below).*
	Special Educational Needs records	Date of birth plus up to 35 years (risk assessed)

	Type of Record/Document	Suggested Retention Period
Safeguarding	Policies, procedures and insurance	Keep a permanent record of historic policies
	DBS disclosure certificates	No longer than 6 months from decision on recruitment, unless police specifically consulted. A record of the checks being made must be kept on SCR / personnel file, but not the certificate itself.
	Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim, and subject to regular review. 35 years for safeguarding records 75 years for child sexual abuse records
	Child Protection files and specific records of child sexual abuse	If a referral has been made / social care has been involved / child has been subject of a multi-agency plan; or if any risk of future claim(s): 75 years.
	Video recordings of one-to-one safeguarding meetings, counselling etc.	A shorter-term retention is acceptable based on the DSL's view / review of how quickly a concern will likely be raised e.g. 3-6 months or immediately.
Accounting Records	Accounting records (records which enable accurate financial position to be ascertained & which give a true and fair view)	Minimum – 6 years for UK charities from the end of the financial year in which the transaction took place
	Tax returns	Minimum of 6 years
	VAT returns	Minimum of 6 years
	Budget and financial reports	Minimum of 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; coexistence agreements; consents)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.

	Type of Record/Document	Suggested Retention Period
Insurance Records	Insurance policies	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	Minium - 7 years (*but this will depend on what the policy covers and whether e.g. historic claims may still be made*)
Employee / Personnel Records *NB these records will contain personal data*	Single Central Record of employees	Keep a permanent record that mandatory checks have been undertaken (but do not keep DBS certificate information itself: 6 months as noted in Safeguarding section)
	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	Potentially permanent (i.e. lifetimes of those involved), depending on nature of scheme
	Job application and interview / rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
	Staff immigration records (Right to Work, etc.)	Minimum - 2 years from end of employment
	Tier 2 migrant worker sponsor records	Minimum - 1 year from end of employment
	Health records relating to employees	7 years from end of employment
	Records of low level concerns about adults	At least until the end of employment, then subject to review: e.g. 7 years from end of employment if they have ongoing relevance for employment claims, longer for safeguarding purposes / claims.

	Type of Record/Document	Suggested Retention Period
Environmental, Health and Data	Maintenance logs	10 years from date of last entry
	Accidents to Children	25 years from birth (longer for safeguarding)
	Accident at work records (staff)	Minium - 4 years from date of accident, but review case by case where possible
	Staff use of hazardous substances	Minimum - 7 years from end of date of use
	Covid-19 risk assessments	Retain (for now) legal paperwork (consents, risk assessments) but not individual test results
	Risk Assessments	7 years from completion of relevant project, incident, event or activity
	GDPR records of processing	No limit (as long as no personal data held) but must be kept up to date, accurate and relevant.

Appendix 2 - Log for destruction of data

File Title / Brief Description of Records Being Disposed of	Retention Period	Covering Dates	Quantity / Number of Volumes	Date Disposed	Name of Staff Disposing Data	Disposal Method (eg shredded, deleted, security waste sack)	Name of Person Destroying / Contractor
e.g. "hirer of facilities application forms"	*current academic year plus 6 years*	*1/9/2012 - 31/8/2013*	*10 forms or 1 folder*	*06/09/2019*	*A N Other*	*Security Waste Sack*	*Sheard Packaging*
e.g. "Hirer of facilities booking forms"	*current academic year plus 6 years*	*01/09/2013 - 31/08/2016*	*30 forms / 3 folders*	*06/09/2022*	*A N Other*	*Deleted off Google*	*A N Other*