



# GDPR Records Management Policy

## Contents:

### [Statement of intent](#)

1. [Legal framework](#)
2. [Responsibilities](#)
3. [Benefits of a retention policy](#)
4. [Retention of pupil records and other pupil-related information](#)
5. [Retention of staff records](#)
6. [Retention of senior leadership and management records](#)
7. [Retention of health and safety records](#)
8. [Retention of financial records](#)
9. [Retention of other school records](#)
10. [Storing and protecting information](#)
11. [Accessing information](#)
12. [Digital continuity statement](#)
13. [Information audit](#)
14. [Disposal of data](#)
15. [Monitoring and review](#)

## Statement of intent

Torquay Girls' Grammar School is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible by the appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR), the school also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The school has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the school's statutory requirements.

This document complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Authorised by:

DPO: N Twelves Date: May 2018

Principal: N Smith Date: May 2018

Financial supervisor: S Wallwork Date: May 2018

## 1. Legal framework

1. This policy has due regard to legislation including, but not limited to, the following:
  - a. General Data Protection Regulation (2016)
  - b. Freedom of Information Act 2000
  - c. Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
2. This policy also has due regard to the following guidance:
  - a. Information Records Management Society 'Information Management Toolkit for Schools' 2016
3. This policy will be implemented in accordance with the following school policies and procedures:
  - a. Data Protection Policy
  - b. Freedom of Information Policy
  - c. E-security Policy

## 2. Responsibilities

1. The school as a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.
2. The **Principal** holds overall responsibility for this policy and for ensuring it is implemented correctly.
3. The **Data Protection Officer (N Twelves)** is responsible for the management of records at **TGGS**.
4. The **DPO** is responsible for promoting compliance with this policy and reviewing the policy on an **annual** basis, in conjunction with the **Principal**.
5. The **DPO** is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy and are disposed of correctly.
6. All **staff members** are responsible for ensuring that any records for which they are responsible for are **accurate, maintained securely and disposed of correctly**, in line with the provisions of this policy.
7. The retention schedule refers to all information, regardless of the media in which they are stored.

## 3. Benefits of a retention schedule

1. Managing records against the retention schedule is deemed to be "normal processing" under the General Data Protection Regulation 2016 and the Freedom of Information Act 2000. Provided members of staff are managing record series using the retention schedule they cannot be found guilty of unauthorised tampering with files once a freedom of information request or a data subject access request has been made.
2. Members of staff can be confident about destroying information at the appropriate time.
3. Information which is subject to Freedom of Information and Data Protection legislation will be available when required.
4. The school is not maintaining and storing information unnecessarily.

## 4. Retention of pupil records and other pupil-related information

- The table below outlines the school's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements.
- Electronic copies of any information and files will be destroyed, through deletion, in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Admissions</b>		
Register of admissions	Three years after the date on which the entry was made	Information is reviewed, and the register may be kept permanently
Secondary school admissions	The current academic year, plus one year	Securely disposed of
Proof of address etc. (supplied as part of the admissions process)	The current academic year, plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Added to the pupil's record	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Until the appeals process has been completed	Securely disposed of
<b>Pupils' educational records</b>		
Secondary Pupils' educational records	25 years after the pupil's date of birth	Securely disposed of
Public examination results	Added to the pupil's educational record	Returned to the examination board
Internal examination results	Added to the pupil's educational record	Securely disposed of
Child protection information held on a pupil's record	Stored in a sealed envelope for the same length of time as the pupil's record	Securely disposed of
Child protection records held in a separate file	25 years after the pupil's date of birth	Securely disposed of

Records/correspondence created in response to serious/ongoing issues with a pupil	Added to the pupil's educational record	Securely disposed of
Records/correspondence created in response to a minor issue with a pupil	Kept by HOD/HOY/SMT in a secure location for the current academic year + 3	Securely disposed of
Records created by teachers/HODs to analyse data and kept outside of SIMS	Current academic year	Securely disposed of. Data trends etc can be kept indefinitely if anonymised.
E-mails containing personal information	Current year unless then need to be added to a pupil's educational record.	Securely disposed of
<b>Attendance</b>		
Attendance registers	Last date of entry on to the register, plus three years	Securely disposed of
Absence notes (kept locked in the attendance officer's office)	Current academic year.	Securely disposed of
Letters requesting/authorising absence	Current academic year, plus two years	Standard disposal
<b>SEND</b>		
SEND files, reviews and individual education plans	25 years after the pupil's date of birth (as stated on the pupil's record)	Information is reviewed and the file may be kept for longer than necessary if it is required for the school to defend themselves in a 'failure to provide sufficient education' case
Statement of SEN maintained under section 324 of the Education Act 1996 or an EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold

Accessibility strategy	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
<b>Curriculum management</b>		
SATs results	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of
External Examination Papers/11+	Until the appeals/validation process has been completed	Securely disposed of
KAWs (named and marked)	Keep for the curriculum year (or longer if HOD requires – max 7 years)	Standard disposal.
Published Admission Number (PAN) reports	Current academic year, plus six years	Securely disposed of
Valued added and contextual data	Current academic year, plus six years	Securely disposed of
Self-evaluation forms	Current academic year, plus six years	Standard disposal unless they have personal data in – then secure disposal
Hard copies of pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Standard disposal. If you want to keep/display then anonymise them.
Online pupils work in their own areas/Office 365	Students to administer their own user areas but kept until they leave.	ICT department will dispose of as they close the account down.
Pupils' work held on shared drives (Student Work/SharePoint etc.)	Staff to clean their parts of these areas at the end of each academic year.	Deleted

Reward evenings/Programs for plays & concerts/headteacher's newsletters etc. As long as the only information is the students' names and their role/prize	One copy to be kept for the school/digitally. Other spares to be disposed of immediately following the event. Parents allowed to take their copy home.	Standard disposal.
<b>Extra-curricular activities</b>		
All information collected for school trips where no major incident occurred	Until the conclusion of the trip	Securely disposed of
All information for school trips where a major incident occurred	25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	Securely disposed of
Walking bus registers	Three years from the date of the register being taken	Securely disposed of
<b>Family liaison officers and home-school liaison assistants</b>		
Day books	Current academic year, plus two years	Reviewed and standard disposal if no longer required
Reports for outside agencies	Duration of the pupil's time at school	Securely disposed of
Referral forms	Whilst the referral is current	Securely disposed of
Contact data sheets/Pastoral reports	Current academic year	Reviewed and secure disposal if no longer active
Contact database entries/Pastoral reports	Current academic year	Reviewed and deleted if no longer required
Pastoral files	25 years after the pupil's date of birth	Securely disposed of



## 5. Retention of staff records

- The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.
- Electronic copies of any information and files will also be destroyed, through deletion, in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Operational</b>		
Staff members' personal file	Termination of employment, plus six years	Securely disposed of
Timesheets	Current academic year, plus six years	Securely disposed of
Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of
<b>Recruitment</b>		
Records relating to the appointment of a new Principal	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file and other information retained for six months	Securely disposed of
DBS certificates	Up to six months	Securely disposed of
Proof of identify as part of the enhanced DBS check	After identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, securely disposed of
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of

### Disciplinary and grievance procedures

<p>Child protection allegations, including where the allegation is unproven</p>	<p>Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer</p> <p>If allegations are malicious, they are removed from personal files</p>	<p>Reviewed and securely disposed of</p>
<p>Oral warnings</p>	<p>Date of warning, plus six months</p>	<p>Securely disposed of – if placed on staff personal file, removed from file</p>
<p>Written warning – level 1</p>	<p>Date of warning, plus 6 months</p>	<p>Securely disposed of – if placed on staff personal file, removed from file</p>
<p>Written warning – level 2</p>	<p>Date of warning, plus 12 months</p>	<p>Securely disposed of – if placed on staff personal file, removed from file</p>
<p>Final warning</p>	<p>Date of warning, plus 18 months</p>	<p>Securely disposed of – if placed on staff personal file, removed from file</p>
<p>Records relating to unproven incidents</p>	<p>Conclusion of the case, unless the incident is child protection related and is disposed of as <u>above</u></p>	<p>Securely disposed of</p>

## 6. Retention of senior leadership and management records

- The table below outlines the school’s retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.
- Electronic copies of any information and files will also be destroyed, through deletion, in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Governing board</b>		
Agendas for governing board meetings	One copy alongside the original set of minutes – all others disposed of without retention	Standard disposal unless personal data then securely disposed of
Original, signed copies of the minutes of governing board meetings	Permanent	
Inspection copies of the minutes of governing board meetings	Date of meeting, plus three years	Shredded if they contain any sensitive and personal information. Destroyed if not
Reports presented to the governing board	Minimum of six years, unless they refer to individual reports – these are kept permanently	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes
Meeting papers relating to the annual parents’ meeting	Date of meeting, plus a minimum of six years	Securely disposed of
Instruments of government, including articles of association	Permanent	
Trusts and endowments managed by the governing board	Permanent	Retained in the school whilst it remains open, then provided to the <b><u>local authority archives service</u></b> when the school closes
Action plans created and administered by the governing board	Duration of the action plan, plus three years	Securely disposed of
Policy documents created and administered by the governing board	Duration of the policy, plus three years	Securely disposed of

Records relating to complaints dealt with by the governing board	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Date of report, plus 10 years	Securely disposed of
Proposals concerning changing the status of the school	Date proposal accepted or declined, plus three years	Securely disposed of
<b>Principal and senior leadership team (SLT)</b>		
Log books of activity in the school maintained by the Principal	Date of last entry, plus a minimum of six years	Reviewed and offered to the <b><u>local authority archives service</u></b> if appropriate
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed and standard disposal unless personal data involved then securely disposed of
Reports created by the Principal or SLT	Date of the report, plus a minimum of three years	Reviewed and standard disposal unless personal data involved then securely disposed of
Records created by the Principal, deputy Principal, heads of year and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed and standard disposal unless personal data involved then securely disposed of
Correspondence created by the Principal, deputy Principal, heads of year and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Reviewed and standard disposal unless personal data involved then securely disposed of
Professional development plan	Duration of the plan, plus six years	Securely disposed of
School development plan	Duration of the plan, plus three years	Securely disposed of

## 7. Retention of health and safety records

- The table below outlines the school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.
- Electronic copies of any information and files will also be destroyed, through deletion, in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Health and safety</b>		
Health and safety policy statements	Duration of policy, plus three years	Standard disposal
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposal
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of <b>15</b> years is applied	Securely disposed of
Accident reporting – adults	Date of the incident, plus six years	Securely disposed of
Accident reporting – pupils	25 years after the pupil's date of birth, on the pupil's record	Securely disposed of
Control of substances hazardous to health	Current academic year, plus 40 years	Standard disposal
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Standard disposal
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Standard disposal
Fire precautions log books	Current academic year, plus six years	Standard disposal

## 8. Retention of financial records

- The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.
- Electronic copies of any information and files will also be destroyed, through deletion, in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Payroll pensions</b>		
Maternity pay records	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
<b>Risk management and insurance</b>		
Employer's liability insurance certificate	Closure of the school, plus 40 years	Securely disposed of
<b>Asset management</b>		
Inventories of furniture and equipment	Current academic year, plus six years	Standard disposal
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of
<b>Accounts and statements including budget management</b>		
Annual accounts	Current academic year, plus six years	Disposed of against common standards
Loans and grants managed by the school	Date of last payment, plus 12 years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of

Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Current financial year, plus six years	Securely disposed of
<b>Contract management</b>		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years	Securely disposed of
All records relating to the management of contracts under signature	Last payment on the contract, plus six years unless longer deemed necessary by the DPO	Securely disposed of
All records relating to the monitoring of contracts	Current academic year, plus two years	Securely disposed of
<b>School fund</b>		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of
<b>School meals</b>		
Free school meals registers	Current academic year, plus six years	Securely disposed of
School meals registers	Current academic year, plus three years	Securely disposed of
School meals summary sheets	Current academic year, plus three years	Securely disposed of
Catering records with biometric data on the NRS system	Biometric data linked to the student so added to their student record (held until 25)	Securely disposed of

## 9. Retention of other school records

- The table below outlines the school's retention periods for any other records held by the school, and the action that will be taken after the retention period, in line with any requirements.
- Electronic copies of any information and files will also be destroyed, through deletion, in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Property management</b>		
Title deeds of properties belonging to the school	Permanent	<b><u>Transferred to new owners if the building is leased or sold</u></b>
Plans of property belonging to the school	For as long as the building belongs to the school	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the school	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of school premises	Current financial year, plus six years	Securely disposed of
<b>Maintenance</b>		
All records relating to the maintenance of the school carried out by contractors or school employees	Current academic year, plus six years unless longer deemed necessary by the DPO	Securely disposed of
<b>Operational administration</b>		
General file series	Current academic year, plus five years	Reviewed and securely disposed of
Records relating to the creation and publication of the school brochure and/or prospectus	Current academic year, plus three years	Reviewed and standard disposal unless personal data involved then securely disposed of
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus one year	Secure disposal
Newsletters and other items with short operational use	Current academic year plus one year	Reviewed and standard disposal unless personal data involved then securely disposed of



Visitors' books and signing-in sheets	Current academic year, plus six years	Reviewed then securely disposed of
Records relating to the creation and management of parent-teacher associations and/or old pupil associations	Current academic year, plus six years	Reviewed then securely disposed of

## 10. Storing and protecting information – Basic principles:

1. The **DPO** will undertake a risk analysis to identify which records are vital to school management and these records will be stored in the most secure manner.
2. The **IT department** will conduct a back-up of information to ensure that online data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.
3. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
4. Confidential paper records are not left unattended or in clear view when held in a location with general access.
5. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up and held in a locked fire safe.
6. Where data is saved on removable storage or a portable device the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use.
7. Memory sticks are not used to hold personal information unless they are password-protected and/or fully encrypted.
8. All electronic devices are password-protected to protect the information on the device in case of theft.
9. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
10. All members of staff are provided with their own secure login and password, and every computer prompts users to change their password.
11. Emails containing sensitive or confidential information are rarely used and if they are they are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.
12. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
13. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
14. Before sharing data, staff always ensure that:
  - They have consent from data subjects to share it.

- Adequate security is in place to protect it.
  - The data recipient has been outlined in a privacy notice (if a third party).
15. All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.
  16. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
  17. The physical security of the school's buildings and storage systems, and access to them, is reviewed **bi-annually** by the **site manager** in conjunction with **the DPO**. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the **Principal** and extra measures to secure data storage will be put in place.
  18. The school takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
  19. The **DPO** is responsible for continuity and recovery measures are in place to ensure the security of protected data.
  20. Any damage to or theft of data will be managed in accordance with the school's **Data Protection Policy/ICO's rules.**

## Accessing information

**TGGS** is transparent with data subjects, the information we hold and how it can be accessed.

All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to provide and withdraw consent to information being held.
- Understand what the school is doing to comply with its obligations under the GDPR.
- All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.
- Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.
- Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.
- The school will adhere to the provisions outlined in the school's **GDPR Data Protection Policy** when responding to requests seeking access to personal information.

## 12. Business continuity statement

Digital data that is retained for longer than six years according to the retention policies will be named as part of a **digital continuity statement**.

- Memory sticks will never be used to store digital data, subject to a digital continuity statement.
- The IT Network Manger will review new and existing storage methods annually and, where appropriate add them to the **business continuity statement in-line** with our GDPR records management policy.

## 13. Information audit

The school conducts information audits on an **annual** basis against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information

The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

The **DPO** is responsible for completing the information audit. The information audit will include the following:

- The school's data needs
- The information needed to meet those needs
- The format in which data is stored
- How long data needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original document

The **DPO** will consult with staff members involved in the information audit process to ensure that the information is accurate.

Once it has been confirmed that the information is accurate, the **DPO** will record all details on the school's **Data Mapping Record**

The information displayed on the **Data Mapping Record** will be shared with the **Principal** to gain their approval.

## 14. Disposal of data

- Where disposal of information is outlined as **standard disposal**, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.
- Where disposal of information is outlined as **secure disposal**, this will be shredded, and electronic information will be scrubbed clean and, where possible, cut. **All staff** will keep a record of all files that needed secure disposal that have been destroyed on the "**Data Deletion Log**". This document can be found in the TGGGS GDPR SharePoint area.
- Where the disposal action is indicated as reviewed before it is disposed, the **DPO** will review the information against its administrative value – if the information should be kept for administrative value, the **DPO** will keep a record of this.
- If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.
- Where information has been kept for administrative purposes, the **DPO** will review the information again after **three** years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every **three** subsequent years.
- Where information must be kept permanently, this information is exempt from the normal review procedures

## 15. Monitoring and review

- This policy will be reviewed on an **annual** basis by the **DPO** in conjunction with the **Principal** – the next scheduled review date for this policy is **May 2019**.
- Any changes made to this policy will be communicated to all members of staff and the governing board.