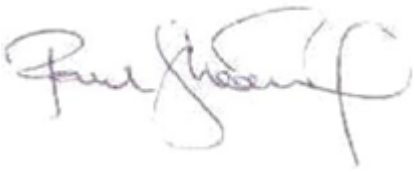
WATFORD GRAMMAR SCHOOL FOR BOYS

DATA RETENTION POLICY

Headmaster's signature 8/5/18

Chair of Governors' signature 8/5/18



School Records Management Policy

Watford Grammar School for Boys

The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

1. Scope of the policy

1.1 This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.
1.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.
1.3 A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service.

2. Responsibilities

2.1 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head of the School.
2.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.
2.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

3. Relationship with existing policies

This policy has been drawn up within the context of:

- Freedom of Information policy
- Data Protection policy
- With other legislation or regulations (including audit, equal opportunities &ethics) affecting the school.

Acknowledgements Content developed in 2012 by: Anthony Sawyer Herefordshire Public Services John Davies TFPL Consultancy

Pupil Records

These guidelines are intended to help provide consistency of practice in the way in which pupil records are managed. These will assist schools about how pupil records should be managed and what kind of information should be included in the file. It is hoped that the guidelines will develop further following suggestions and comments from those members of staff in schools who have the most contact with pupil records.
These guidelines apply to information created and stored in both physical and electronic format.
These are only guidelines and have no legal status, if you are in doubt about whether a piece of information should be included on the file please contact the Local Authority.

Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System
The pupil record should accompany the pupil to every school they attend and should contain information that is accurate, objective and easy to access. These guidelines are based on the assumption that the pupil record is a principal record and that all information relating to the pupil will be found in the file (although it may spread across more than one file cover).

Disclosure

Staff should be made aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it.
Ensure that where you intend to share personal information with a third party that you have considered the requirements of the GDPR.

Safe disposal of records which have reached the end of their administrative life

NB: Please be aware that this guidance applies to all types of record, whether they are in paper or digital format.

1. Disposal of records that have reached the end of the minimum retention period allocated

GDPR principle states that: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

In each organisation, local records managers must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed.
The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the organisation for research or litigation purposes.

Refer to the Retention Guidelines at the end of the toolkit.

Whatever decisions are made they need to be documented as part of the records management policy within the organisation.

2. Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.
• Paper records should be shredded using a cross-cutting shredder
• CDs / DVDs / Floppy Disks should be cut into pieces
• Audio / Video Tapes and Fax Rolls should be dismantled and shredded
• Hard Disks should be dismantled and sanded

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

1. Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.
It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.
2. Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a Senior Manager and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

Freedom of Information Act 2000 (FoIA 2000)

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction

Members of staff should record at least:
• File reference (or other unique identifier);
• File title (or brief description);
• Number of files and date range
• The name of the authorising officer
• Date action taken

Following this guidance will ensure that the school is compliant with the GDPR 2018, Data Protection Act 1998 and the Freedom of Information Act 2000.

Transfer of records to the Archives

Where records have been identified as being worthy of permanent preservation arrangements should be made to transfer the records to the County Archives Service.

The school should contact the local record office if there is a requirement to permanently archive the records, and the records will continue to be managed via the GDPR 2018 and the FoIA 2000. If you would like to retain archive records in a special archive room in the school for use with pupils and parents please contact the local record office for specialist advice.

Digital Continuity

The long term preservation of digital records is more complex than the retention of physical records. A large number of organisations create data in electronic format which needs to be retained for longer than 7 years. If this data is not retained in accessible formats the organisation will be unable to defend any legal challenge which may arise. In order to ensure that digital records are retained in a way that ensures they can be retrieved in an accessible format when they are required, all records which are required to be retained for longer than 6 years should be part of a digital continuity statement. The average life of a computer system can be as little as 5 years, however, as digital continuity is resource intensive, only records which are required to be retained for 6 years (in line with the Limitation Act 1980) or longer should be subject to digital continuity statements.

8.1 The Purpose of Digital Continuity Statements

A digital continuity statement will not need to be applied to all the records created by the school. The retention schedule should indicate which records need to be subject to a digital continuity statement. Any record which needs to be preserved for longer than 6 years needs to be subject to a digital continuity statement. Appropriate records need to be identified as early in their lifecycle as possible so that the relevant standards can be applied to them and conversely any records which do not need to be included in the policy should also be identified in the early part of the lifecycle. Digital continuity statements should only be applied to principal copy records.

8.2 Allocation of Resources

Responsibility for the management of the digital continuity strategy, including the completion of the digital continuity statements should rest with one named post holder. This will ensure that each information assets is “vetted” for inclusion in the strategy and that resources are not allocated to records which should not be included in the strategy.

8.3 Storage of records

Where possible records subject to a digital continuity statement should be “archived” to dedicated server space which is being backed up regularly. Where this is not possible the records should be transferred to high quality CD/DVD, if they are to be included with paper documentation in a paper file or onto an external hard drive which is clearly marked and stored appropriately. Records stored on these forms of storage media must be checked regularly for data degradation. Flash drives (also known as memory sticks) must not be used to store any records which are subject to a digital continuity statement. This storage media is prone to corruption and can be easily lost or stolen. Storage methods should be reviewed on a regular basis to ensure that new technology and storage methods are assessed and where appropriate added to the digital continuity policy

8.4 Migration of Electronic Data

Migration of electronic data must be considered where the data contained within the system is likely to be required for longer than the life of the system. Where possible system specifications should state the accepted file formats for the storage of records within the system. If data migration facilities are not included as part of the specification, then the system may have to be retained in its entirety for the whole

retention period of the records it contains. This is not ideal as it may mean that members of staff have to look on a number of different systems to collate information on an individual or project. Software formats should be reviewed on an annual basis to ensure usability and to avoid obsolescence.

8.5 Degradation of Electronic Documents

In the same way as physical records can degrade if held in the wrong environmental conditions, electronic records can degrade or become corrupted. Whilst it is relatively easy to spot if physical records are becoming unusable it is harder to identify whether an electronic record has become corrupted, or if the storage medium is becoming unstable. When electronic records are transferred from the main system to an external storage device, the data should be backed up and two safe copies of the data should be made. The data on the original device and the back-ups should be checked periodically to ensure that it is still accessible. Additional back-ups of the data should be made at least once a year and more frequently if appropriate. Where possible digital records should be archived within a current system, for example, a designated server where “archived” material is stored or designated storage areas within collaborative working tools such as SharePoint.

8.6 Internationally Recognised File Formats

Records which are the subject of a digital continuity statement must be “archived” in one of the internationally recognised file formats.

8.7 Digital Continuity Strategy Statement

1. Statement of business purpose and statutory requirements for keeping records

The statement should contain a description of the business purpose for the information assets and any statutory requirements including the retention period for the records. This should also include a brief description of the consequences of any loss of data. By doing this the records owner will be able to show why and for how long the information assets needs to be kept. As digital continuity can be resource intensive, it is important that the resources are allocated to the information assets which require them.

2. Names of the people/functions responsible for long term data preservation

The statement should name the post-holder who holds responsibility for long term data preservation and the post holder responsible for the information assets. The statement should be updated whenever there is a restructure which changes where the responsibility for long term data preservation is held. If the responsibility is not clearly assigned there is the danger that it may disappear as part of a restructure process rather than be reassigned to a different post.

3. Description of the information assets to be covered by the digital preservation statement

A brief description of the information asset

4. Description of when the record needs to be captured into the approved file formats

The record may not need to be captured in to the approved file format at its creation. For example, an MSWord document need not be converted to portable document format until it becomes semi-current.

The digital preservation statement should identify when the electronic record needs to be converted to the long term supported file formats identified above. Workflow process diagrams can help identify the appropriate places for capture.

5. Description of the appropriate supported file formats for long term preservation

This should be agreed with the appropriate technical staff. Information Management Toolkit for Schools Version 4 – July 2012 43

6. Retention of all software specification information and licence information

Where it is not possible for the data created by a bespoke computer system to be converted to the supported file formats, the system itself will need to be mothballed. The statement must contain a complete system specification for the software that has been used and any licence information which will allow the system to be retained in its entirety. If this information is not retained it is possible that the data contained within the system may become inaccessible with the result that the data is unusable with all the ensuing consequences

7. Description of where the information asset is to be stored.

See section 4 above

8. Description of how access to the information asset is to be managed within the data security protocols

The data held for long term preservation must be accessible when required but also must be protected against the standard information security requirements which are laid down for records within the authority. The statement must contain the policy for accessing the records and the information security requirements attached to the information assets.