Records Management

**Introduction**

This document sets out how the College records management system works. It predominantly refers to paper files, but electronic files also need to be regularly reviewed. It should be used in conjunction with the Records Retention Schedule (RRS). Please contact the Records Management Officer if you have any questions or queries.

The more information stored in an office or on a computer, the more difficult it becomes to find the relevant piece of information. In order to ensure maximum efficiency, non-current material should be removed at regular intervals. This booklet explains which records should be kept, and what to do with them once they are no longer current.

**Types of Record**

**Current**

Current records are those still in regular use. They are files which are either consulted or added to on a regular basis. These should be kept in the filing cabinets, shelves or drawers in the office, on the shared Departmental drive, or on ModGov.

**Semi-current**

These are records which are no longer used regularly, but which need to be kept either for legal reasons or occasional use. They should be kept physically separate from current records in the office, or in a separate folder on the computer.

**Inactive**

These records are no longer needed for administrative use, and have come to the end of any applicable legal retention periods. These need to be either transferred to the Archive for long term preservation or destroyed. Note that a record should be kept of any files destroyed.

**The Records Retention Schedule (RRS)**

A department’s RRS should list all the records which are produced by the department, and will state what should happen to those records once no longer required by the department. If there are any significant changes to the department’s working practices and the records it produces, the department should liaise with the Records Management Officer to update the RRS accordingly. Some records, such as committee minutes and general departmental records may be held by any department.

**Reviewing Records**

Records should be reviewed on a regular basis, either once or twice a year, depending on the volume of records produced.

**Paper Records**

Any paper files no longer regularly needed may be transferred either to a Semi-Current Record Store (SCRS), transferred to the Archives, or destroyed. The RRS sets out retention periods and final action on files. If a record is to be destroyed, then the Head of Department will need to complete a ‘Record Destruction Form’. Records which contain personal or sensitive data, such as home addresses, dates of birth, comments about students or staff, or copies of committee minutes must be confidentially destroyed. Note that confidential paper disposal sacks must be kept securely until disposed. Printed circulars and records containing no sensitive data should be recycled.

**Electronic Records**

Electronic records (both on personal drives and on departmental shared drives) must also be reviewed periodically. Those which might be of continuing (archival) value should be located, and the Archivist contacted to discuss ways of transferring the records to a digital long-term storage area. Records that are of no further use should be deleted, especially early drafts of documents and committee minutes (excluding the copies kept by the Chair, Convener or Secretary). Deletion of electronic records, excluding drafts and working documents, should be treated in the same way as the destruction of paper records and a ‘Record Destruction Form’ must be completed. For example, the deletion of order letters or contracts at the end of their retention period should be treated the same as shredding a physical copy. The deletion of draft minutes, general e-mail correspondence, or other working documents does not require a record destruction form.

**Requesting a Current or Semi-Current file**Departments have control of their own current and semi-current files. Should a record need to be viewed by a member of staff outside the department in which it was created, permission must be given by the relevant Head of Department in accordance with the Data Protection Policy. Files should be handed over in person, both when sending and when receiving.

**Note:** While a different department has the physical copy of a file, they must follow the same security and/or confidentiality procedures as the file would normally be subject to.

**Legislation**

**Data Protection Act 1998**The Data Protection Act 1998 works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles which make sure that personal information is:

• Fairly and lawfully processed;

• Processed for limited purposes;

• Adequate, relevant, and not excessive;

• Accurate and up to date;

• Not kept longer than is necessary;

• Processed in line with the individual’s rights;

• Kept securely; and

• Not transferred to other countries without adequate protection.[[1]](#footnote-1)

Secondly, it gives people a right to see the data that is held about them by an organisation. The information can be in any format, e.g. emails or reports, and can be held by any member of the organisation. The Freedom of Information Act 2000 amends the Data Protection Act 1998 in a number of ways, including extending data subjects’ right of access to personal information held about them by the College. From 2005 individuals have the right to access personal information held in ‘unstructured’ files, so that even personal data held in a file relating to something else (eg a file without the subject’s name on the front or minutes of a meeting) will be covered by the Data Protection Act 1998. When handling personal data you need to think about how you are using it and storing it. You should be aware of who has access to the data and always ensure it is kept safely and securely. All data protection enquiries or requests for personal information should be passed to the Bursar as the College’s Data Protection Officer.

**Freedom of Information Act 2000**The Freedom of Information Act 2000 gives a general right of access to recorded information held or created by the College. The Act sets out the exemptions to disclosure and the way that requests for information should be handled. All requests made for information should be forwarded to the Bursar as the College’s Freedom of Information Officer. Some information, including personal details held under the Data Protection Act 1998, will be exempt and will not need to be disclosed. The records management programme ensures that the College has a sound basis for handling requests. However, members of staff must adhere to the Records Retention Schedule and advise the Records Management Officer of any changes to record-keeping in order to comply with legislation.

**More Information**

Data Protection Act 1998

<http://www.legislation.gov.uk/ukpga/1998/29/contents>

Freedom of Information Act 2000

<http://www.legislation.gov.uk/ukpga/2000/36/contents>

The Secretary of State for Constitutional Affairs’ Code of Practice on the Discharge of Public Authorities Functions under the Freedom of Information Act 2000

<http://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf>

The Information Commissioner’s Website for General Information about both the Data Protection Act 1998 and the Freedom of Information Act 2000

<http://www.ico.gov.uk/>

Freedom of Information at Newnham College

<http://www.newn.cam.ac.uk/about/freedom-of-information/>

Data Protection at Newnham College

<http://www.newn.cam.ac.uk/alumnae/keeping-in-touch/data-protection/>

**Contacts**

Archivist Email: archives@newn.cam.ac.uk

Ms Anne Thomson Phone: 35738

 Freedom of Information Officer Email: bursar@newn.cam.ac.uk

 Mr Donald Hearn, Bursar Phone: 35750

Data Protection Officer Email: bursar@newn.cam.ac.uk

 Mr Donald Hearn, Bursar Phone: 35750

**Last updated 11 May 2018**

**Donald Hearn**

**Bursar, Newnham College**

1. https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/ [↑](#footnote-ref-1)