CTF Data Protection Policy
How we use your personal information (for staff)

Data Protection Act 1998 (DPA): How we use your personal information

1. What is 'personal information'?  
'Personal information' means any information which identifies you as an individual.

2. Who the policy applies to  
This policy applies to all staff employed by the Cambridge Theological Federation.

3. Why the policy is needed  
The Cambridge Theological Federation is committed to a policy of protecting the rights and privacy of its employees, in accordance with the Data Protection Act. The Cambridge Theological Federation needs to process certain information about its employees for administrative purposes (e.g. – to recruit and pay staff). The information published here applies to the processing of your personal information by the Cambridge Theological Federation (“the Federation”). Please note that the Federation and each of the Federation houses are separate legal entities in data protection terms.

4. The policy principles

Policy Statement  
To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed unlawfully to any third party (without the express consent of the individual).

Any breach of the Data Protection Act 1998 by staff is considered to be an offence and if that occurs, The Cambridge Theological Federation Disciplinary Policy will apply. As a matter of good practice, other individuals working with The Cambridge Theological Federation, who have access to personal information, will be expected to have read and comply with this policy.

All processing of personal data must be done in accordance with the eight data protection principles.

- Personal Data must be processed fairly and lawfully.

  Those responsible for processing personal data must make reasonable efforts to ensure that staff are informed of the identity of the data controller (in this case The Cambridge Theological Federation), the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

- Personal Data shall be obtained for specific and lawful purposes and not processed in a way which is incompatible with these purposes.

- Personal Data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.
Information which is not strictly necessary for the purpose for which it is obtained should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

- Personal Data should be accurate and where necessary kept up to date.

Data which has been kept for a long time should be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume it is accurate. It is the responsibility of staff to ensure that data is accurate and kept up to date. Staff should notify The Cambridge Theological Federation of any changes to ensure personal records are updated.

- Personal data should only be kept for as long as is necessary. (See “Retention and Disposal of Data”).

- Personal data should be processed in accordance with the rights of employees (data subjects) under the Data Protection Act.

The Cambridge Theological Federation must comply with requests for access to data from employees.

- The Cambridge Theological Federation needs to take measures to ensure the security and confidentiality of Personal Data. (See section on “Security of Data”).

- Personal Data should not be transferred to any country outside of the European Economic Area, unless that an adequate level of data protection is ensured.

Rights of Employees (Data Subjects)

Under the Data Protection Act the employee has the following rights:

- To access any Personal Data which The Cambridge Theological Federation holds. If an employee wishes to access his or her personal data he or she must make a written request (a fee may be charged at the discretion of The Cambridge Theological Federation to cover administrative costs). The Cambridge Theological Federation will normally respond within 40 days of this request.
- To prevent the processing of Personal Data if it is likely to cause damage or distress.
- To take action to rectify, block, erase or destroy any inaccurate data which is held by The Cambridge Theological Federation.

Right to Privacy: What right to privacy does an employee have?

At the moment an employee does not have a free-standing right to privacy. However, in the context of the Data Protection Act and the Human Rights Act 1998 it is clear that the employee does have some rights to privacy within the workplace.

5. The definition of terms used in the document

Definitions:
• ‘Data Controller’: any person (or organisation) who makes decisions in connection with personal data, including decisions regarding the purposes for which personal data is processed and the way in which that data is processed.

• ‘Data Subject’: any individual who is the subject of personal data held by an organisation.

• ‘Personal Data’: data relating to an individual who can be identified from that information. This includes name, address, telephone number etc.

• ‘Sensitive Personal Data’: different from ordinary personal data (see above) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual orientation and criminal convictions. Sensitive data is subject to much stricter conditions of processing.

• ‘Processing’: this covers nearly everything from the storage of data in any form, copying, checking and sorting, through to its deletion.

• ‘Third Party’: any individual/organisation other than the data subject and the data controller (The Cambridge Theological Federation).

6. How the policy will be applied

The Human Rights Act states that everyone has the right to respect for their private and family life, their home and their correspondence. However, it may be acceptable to override this right if it is in accordance with the law and for the reasons given below under “Disclosure of Data”.

What right do I have to access of information?

• Under the rules of the Data Protection Act 1998, individuals are allowed to view certain information held about them.

• In relation to references, medical records and disciplinary records, employees can request to see the information that is kept on them.

• The Cambridge Theological Federation will use its discretion to disclose information as far as it is reasonably practicable to do so. In certain circumstances, in order to protect the rights of a third party, it may not be appropriate to do so.

Security of Data

All employees are responsible for the data they hold on other people. They must ensure that the data is kept securely and not disclosed to a third party (see “Disclosure of Data”).

To ensure that personal data is kept securely it should be kept:

• In a lockable room with controlled access; or
• In a locked drawer or filing cabinet; or
• If computerised, it should be password protected; or
• Kept on disks which should also be kept securely.

Care should be taken to ensure that computers are not visible to unauthorised staff and that computer passwords are kept confidential. Computer screens should not be left unattended without being password protected and manual records should not be left where they can be accessed by unauthorised employees.

Particular care should be taken when personal data is used at home or in other locations outside of The Cambridge Theological Federation.
Disclosure of Data

All staff must ensure that personal data is not disclosed to unauthorised third parties. This includes family members, friends and government bodies.

Personal data may be disclosed where one of the following conditions applies:

- The individual has given his or her consent;
- Where the disclosure is legitimate (e.g. – disclosure to other staff if they require it to perform their jobs); or
- Where The Cambridge Theological Federation has legally to disclose the data (e.g. – equal opportunities monitoring).

The Data Protection Act also allows disclosures without consent as long as the information is requested for one or more of the following purposes:

- To prevent or detect a crime;
- In the interests of national security;
- In the interests of public safety;
- To protect the interests of the individual (this refers to life and death situations); or
- To protect the rights and freedom of others (which include The Cambridge Theological Federation).

Unless consent has been obtained, information should not be given out over the telephone. As an alternative, staff may offer to do the following:

- Pass a message to the individual asking them to contact the enquirer; or
- Accept a sealed envelope/email message and try to forward it to the individual.

If there is any doubt staff should seek advice from their line manager.

Retention and Disposal of Data

The Cambridge Theological Federation discourages personal data to be kept for longer than it is required.

In general, staff records containing information including names and addresses, positions held and leaving salaries are kept indefinitely. Other information relating to staff members will be kept by for The Cambridge Theological Federation 6 years from the end of employment.

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date.

Personal data must be disposed of in a way that protects the rights and privacy of individuals. This includes shredding or secure electronic deletion.

Non-personal data should be used sensitively and only given to the necessary parties. The length of time that records should be kept for is down to the individual’s own discretion and their common sense. It is dependent on the actual information and circumstances.
7. **Responsibility for administering and updating the policy**

The Registrar is responsible for updating this policy in consultation with the President of the Federation Management Committee, seeking advice as necessary.

8. **Higher Education statistics Agency (HESA)**

HESA collection notices provide information to students and staff about what happens to their data when it is sent to HESA. Provision of the relevant collection notice is necessary to comply with the first Principle of the Data Protection Act. The HESA data protection guidance note is available at [https://www.hesa.ac.uk/index.php?option=com_content&view=article&id=141&Itemid=171#Staff](https://www.hesa.ac.uk/index.php?option=com_content&view=article&id=141&Itemid=171#Staff)

9. **When the policy was last revised, when it will next be revised.**

July 2016
July 2019

10. **The date from which it applies**

July 2016

11. **Statutory regulations and good practice guidance**

**Data Protection Act 1998**
The purpose of the Data Protection Act is to protect the rights and privacy of individuals and to ensure that personal data is not processed without their knowledge and wherever possible is processed with their consent.

**Human Rights Act 1998**

**Schedule One**

**Responsibilities under the Data Protection Act:**

**Responsibilities of The Cambridge Theological Federation**

- Under the terms of the Data Protection Act The Cambridge Theological Federation is the Data Controller (see definitions above).
- The Cambridge Theological Federation is committed to protecting the right of individuals to privacy with respect to the processing of their personal data.
- All those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within The Cambridge Theological Federation.

**Responsibilities of Staff (Employees)**

- Staff are responsible for the security of the data they process and for ensuring that it is not disclosed to anyone who is not entitled to it.
- Staff are also Data Subjects (see definitions above) and should ensure, therefore, that any information they supply to The Cambridge Theological Federation is accurate and up to date.
The Cambridge Theological Federation cannot be held responsible for any errors arising from changes about which it has not been informed.

Further Information

Information Commissioner’s Webpage - http://www.ico.gov.uk/

ACAS - http://www.acas.co.uk/

Approved by the Federation Management Committee 12th July 2016

DATA PROTECTION: How we use your personal information (for students)

Information Compliance

Data Protection Act 1998 (DPA): How we use your personal information

1. What is 'personal information'?
'Personal information' means any information which identifies you as an individual.

2. Who uses my personal information?
The information published here applies to the use, sharing and disclosure of your personal information by the Cambridge Theological Federation (“the Federation”) and by any of the Federation’s constituent member houses and colleges (“the Federation houses”). Please note that the Federation and each of the Federation houses are separate legal entities in data protection terms. The Federation and the individual Federation houses work together closely and share your personal information for a variety of academic, administrative and statistical purposes in accordance with agreed protocols. Your Federation house may provide you with an additional statement about how it will use, share and disclose your personal information (including any information you provide relating to your medical history).

3. How is my personal information used while I’m a student?
Your personal information is created, stored and transmitted securely in a variety of paper and electronic formats, including databases that are shared between the Federation and the Federation houses. Access to your personal information is limited to staff who have a legitimate need and interest in it for the purpose of carrying out their contractual duties.

Your personal information is used as permitted or required by law and for a range of academic and administrative purposes, including the following:

- To facilitate your education, record the details of your academic studies (including any placements with external organisations) and determine your examination achievements.
- To administer the financial aspects of your relationship with us and any funders.
- To manage your use of facilities and participation at events (e.g. computing, libraries, accommodation, functions).
- To enable effective communications with you.
- To operate security, disciplinary, complaint, and quality assurance processes and arrangements.
- To support your training, health, safety and welfare requirements.
To produce statistics and research for internal and statutory reporting purposes.
To monitor our responsibilities under equalities legislation.

Some of the personal information used for the above purposes is classed as 'sensitive personal data' under the DPA, such as information relating to your ethnicity or your medical history. This is collected to monitor our equalities responsibilities and so that staff can be made aware as appropriate of any medical needs. Access to, and the sharing of, this information is controlled very carefully. You will be given more details about our use of any sensitive personal data when we collect it from you.

4. Who is my personal information shared with?

Your personal information is disclosed as permitted or required by law and on a considered and confidential basis to a range of external organisations, including the following:

- Higher Education Statistics Agency (see the details published at http://www.hesa.ac.uk/collection-notices)
- Your funders and/or sponsors
- The providers of any external learning or training placements
- Relevant Government Departments (e.g. Department for Business, Innovation and Skills, Home Office, Foreign and Commonwealth Office, Department of Health, Department for Education)
- Relevant executive agencies or non-departmental public bodies (e.g. UK Visas and Immigration, HM Revenue and Customs, the Health and Safety Executive)
- Higher Education Funding Council for England (HEFCE)
- Universities and Colleges Admissions Service (UCAS)
- Office for Fair Access (OFFA)
- Office of the Independent Adjudicator (OIA)
- The Federation Student Forum
- The organisation(s) running the National Student Survey
- Providers of anti-plagiarism software
- Student Loans Company
- Any relevant professional or statutory regulatory bodies (e.g. Ministry Division, your sponsoring church)
- Local authorities. (In particular, we pass lists of students to the City Council on an annual basis to assist with the administration of students’ exemption from Council Tax)
- The police and similar law enforcement agencies
- Auditors
- Companies or organisations providing specific services on behalf of the Federation and/or one or more Federation houses

Your basic contact details (name, email address and Federation house) will be made available through our internal online directory.

We will not normally disclose any other personal information about you to other external enquirers or organisations without your consent unless it is in your vital interests to do so (e.g. in an emergency situation).

5. How is my personal information used after I graduate?
After you graduate a core record of your studies is retained indefinitely so that the details of your academic achievements can be confirmed and for statistical or historical research. Your contact and core personal details are added to the Federation’s alumni database. Graduates may also be invited to take part in the Destinations of Leavers from Higher Education Survey (DLHE): all responses to DLHE will be treated in accordance with the requirements and guidance of the Higher Education Statistics Agency.

6. How can I access my personal information?
Under the DPA you have the right, subject to certain exemptions, to access the personal information that is held about you. Contact your House or the Office of the Registrar (ctfreg@hermes.cam.ac.uk) for more information.

7. Who regulates the use of my personal information?
The Federation maintains a data protection registration with the Information Commissioner’s Office, the independent authority which oversees compliance with the DPA and sets out, in very general terms, the full range of purposes for which we use student, staff and all other personal information (see https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/).

8. Who do I contact with questions?
Contact the office of the Registrar (ctfreg@hermes.cam.ac.uk) or your House If you have any questions about how your personal information is used.

9. Are changes made to this webpage?
This webpage was last updated in July 2016. It is reviewed when necessary and at least annually. Any changes will be published here and you will be notified via this webpage and/or by email.

10. HESA data protection notice
The Higher Education Statistics Agency (HESA) is the official agency for the collection, analysis and dissemination of quantitative information about higher education.

If you are studying on an award-bearing course we will send some of the information we hold about you to HESA. This information forms your HESA record, which does not include your contact details. Your contact details may be passed to survey contractors to carry out the National Student Survey and surveys of student finances, on behalf of the education organisations listed on the HESA website. These organisations and their contractors will use your details only for that purpose, and will then delete them. For further details see http://www.hesa.ac.uk/collection-notices

Data Retention Policy

1. Introduction
The Cambridge Theological Federation holds a great deal of important information that is crucial to its effective operation. Whilst many information systems can be recovered after an incident, the business critical data that is held in electronic and paper format must be suitably protected. Retention of specific documents may be necessary to:

• fulfill statutory or other regulatory requirements
• evidence events/agreements in the case of disputes
• meet operational needs
• ensure the preservation of documents of historic or other value

The untimely loss or destruction of documents could cause the Federation:

• operational problems
• difficulty in defending litigious claims
• reputational damage
• failure to comply with the Data Protection Act 1998

Conversely, the permanent retention of all documents is undesirable, and appropriate disposal is to be encouraged to:

• avoid unnecessary/excessive use of storage space (electronic or physical)
• comply with legislation regarding the indefinite retention of personal data
• reduce the impact of fire risk (in the case of paper records)
• keep records and office accommodation de-cluttered

Good practice in records management emphasises the importance of organisations having in place systems for the timely and secure disposal of documents/records that are no longer required for business purposes.

This policy will be reviewed and updated regularly to ensure that it remains appropriate in the light of any changes to legal, contractual or acceptable use obligations.

The information published here applies to the retention of data and documentation held by the Cambridge Theological Federation (“the Federation”) and by any of the Federation’s constituent member houses and colleges (“the Federation houses”). The Federation and each of the Federation houses are separate legal entities in terms of data retention and protection. The Federation and the individual Federation houses work together closely for a variety of academic, administrative and statistical purposes in accordance with agreed protocols.

2. Objective
The purpose of this policy is to provide an organisation-wide policy framework to govern management decisions on whether a particular document (or set of documents, including electronic versions) should either be:

• retained – and if so, in what format, and for what period
• disposed of - and if so, when, and by what method

For the avoidance of any doubt, this policy is not concerned with the disposal/retention of unused materials (e.g. stocks of paper, unused forms, duplicated documents and so on).

3. Scope
In the course of carrying out its various functions and activities, the Federation collects information from individuals and external organisations and generates a wide range of data and information which is recorded and stored, both as physical paper records and/or in electronic form. These records can take many different forms, such as:

• completed application forms
• personal details relating to health and/or disability
• student records  
• student assessment  
• examination results  
• confidential minutes of committee meetings  
• contracts  
• identification documents  
• letters received from third parties  
• copy letters which have been sent out  
• personnel records  
• invoices  
• financial records  
• contact details  
• email communications and attachments  
• photos

4. Principles
Staff, students and members of the Federation must comply with the following data protection principles. Data collected by or on behalf of the Federation must be:

1. Fairly and lawfully processed; in particular that the individual whose information it is has consented to the processing of his or her personal information.

2. Processed for limited purposes and only for the purposes for which it was originally supplied. Federation staff and the Federation’s constituent Houses receiving personal information from individuals are obliged to ensure such individuals are fully aware of what we will use this information for. Staff should NOT assume that the provision of personal information gives the Federation the right to use that information for any purpose.

3. Adequate, relevant and not excessive.

4. Accurate and up to date.

5. Not kept longer than is necessary. Personal information should only be retained by the Federation for as long as is required to fulfil the purposes for which it was originally provided. Beyond this point it should be securely destroyed. Please see the Federation’s retention schedule for guidelines on how long certain types of information should be kept.

6. Processed in accordance with the individual’s rights – that is, not to do anything with the information which would prejudice the rights of the individual in any way.

7. Secure. From the point at which personal information is received until the point at which it is destroyed, such information must be processed securely. Federation staff and Houses are obliged to ensure they have appropriate mechanisms in place to ensure adequate security for the storage and transmission of all electronic and paper records containing personal information, particularly more sensitive personal information. BE AWARE that the loss, disclosure or unplanned destruction of personal information can lead to legal action being taken against the Federation.

8. Not transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection.

5. Policy Statement
The Federation is committed to protecting the security of data through preserving:

• confidentiality: protecting information from unauthorised use or disclosure

• integrity: safeguarding the accuracy and completeness of information and processing methods

• availability: ensuring that information is available to authorised users when required
The Federation will develop, implement and maintain its Data Retention Policy to ensure data is adequately stored, processed, transmitted and destroyed in a way consistent with our legal, contractual and ethical obligations.

You may request copies of personal data kept by the Federation in accordance with the retention policy stated below. At the end of the retention period, data are either destroyed or anonymised and used for statistical analyses, unless subject to an appeal or complaint.

All applications for copies of personal data held by the Federation should be directed in writing to the Registrar (ctfreg@hermes.cam.ac.uk). Please note however, that there is no requirement to supply copies of examination scripts under the Data Protection Act of 1998.

Release of data under this policy does not constitute a subject access request under the Data Protection Act of 1998. Requests for access to all other personal data should be directed to the Federation’s Registrar: ctfreg@hermes.cam.ac.uk

6. Retention and disposal protocol

<table>
<thead>
<tr>
<th>Data relating to examination papers and dissertations</th>
<th>Retention time (unless a student has already initiated an appeal against his or her result)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examination scripts and dissertations</td>
<td>Six months from the publication of final results ¹ ²</td>
</tr>
<tr>
<td>Marks for individual questions (examination papers only)</td>
<td>One month from the publication of final results</td>
</tr>
<tr>
<td>Examiners’ comments relating to procedural or rubric infringements or other practical points</td>
<td>One month from the publication of final results</td>
</tr>
<tr>
<td>Examiners’ comments relating to academic judgement</td>
<td>One month from the publication of final results</td>
</tr>
<tr>
<td>Minutes of examiners’ meetings</td>
<td>Indefinitely</td>
</tr>
<tr>
<td>Final result and/or mark or grade</td>
<td>Indefinitely</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data relating to assignment assessment</th>
<th>Retention time (unless a student has already initiated an appeal against his or her result)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment scripts</td>
<td>Two academic years after the academic year of the course ¹ ²</td>
</tr>
<tr>
<td>Assignment grades and/or mark and assignment feedback from tutor</td>
<td>Two academic years after the academic year of the course</td>
</tr>
<tr>
<td>Minutes of examiners’ meetings</td>
<td>Indefinitely</td>
</tr>
<tr>
<td>Final result and/or mark or grade</td>
<td>Indefinitely</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data relating to complaints and appeals procedure</th>
<th>Retention time</th>
</tr>
</thead>
<tbody>
<tr>
<td>All documents relating to students’ appeals and complaints</td>
<td>Six years after the issue of a letter of completion</td>
</tr>
</tbody>
</table>

¹ Assignments unsuitable for electronic submission or scanning will be returned to/collected by you for appropriate retention/storage.
² Occasionally we may wish to keep examples of student work for use in staff development, quality assurance or as a teaching tool. You can opt-out by ticking the box on the Assignment Cover Sheet. In all cases, work will be anonymised.
Copyright and all other intellectual property rights relating to assignments and dissertations remain throughout with you.

**HESA data protection notice**
The Higher Education Statistics Agency (HESA) is the official agency for the collection, analysis and dissemination of quantitative information about higher education.
If you are studying on an award-bearing course we will send some of the information we hold about you to HESA. This information forms your HESA record, which does not include your contact details. Your contact details may be passed to survey contractors to carry out the National Student Survey and surveys of student finances, on behalf of the education organisations listed on the HESA website. These organisations and their contractors will use your details only for that purpose, and will then delete them. For further details see [www.hesa.ac.uk/fpn](http://www.hesa.ac.uk/fpn).

**Document retention and archiving policy**

1. **The retention/disposal protocol**
Any decision whether to retain or dispose of a document should be taken in accordance with the retention/disposal protocol. This protocol consists of:

   - The key disposal/retention considerations criteria checklist, set out in Appendix II. Essentially no document should be disposed of unless all these have been considered in relation to the document.
   - The Retention Schedules (taken from the Records Management Society) contained in Appendix 2. These provide guidance on recommended and mandatory minimum retention periods for specific classes of documents/records.

Where a retention period has expired in relation to a particular document a review should always be carried out before a final decision is made to dispose of that document. Such reviews need not necessarily be detailed or time consuming.

In the event that a decision is taken to dispose of a particular document or set of documents, then consideration should be given to the method of disposal (see section 2 below).

2. **Disposal of documents/records**
A separate policy describes the Federation’s policy regarding secure disposal of confidential information.

As guidance however, staff should take into account the following considerations when selecting any method of disposal:

   - Under no circumstances should paper documents or removable media (CDs, DVDs, discs, etc.) containing personal data or confidential information be simply binned or deposited in refuse tips. To do so could result in the unauthorised disclosure of such information to third parties, and render the Federation liable to action under the Data Protection Act. Such documents should be destroyed on site (e.g. by shredding) or placed in “Confidential Waste” refuse bins.
   - Deletion – the Information Commissioner’s Office has advised that if steps are taken to make data virtually impossible to retrieve, then this will be regarded as equivalent to deletion.
   - Recycling – wherever practicable disposal should further recycling, in line with the
Federation’s commitment to the environment.


Staff should be aware that under the Data Protection Act personal data processed for any purpose must not be kept for longer than is necessary for that purpose. In other words, retaining documents or records that contain personal data beyond the length of time necessary for the purpose for which that data was obtained is unlawful.

The Data Protection Legislation contains no interpretive provisions on this provision. It is a matter for reasonable judgement and common sense as to how long personal data should be retained. Clearly, in many instances the retention of personal data will be necessary and thus justified for a significant period of time. In general, provided there is adherence to this Policy, few problems should arise.

4. How long should I store emails?

Not only does the storage of large numbers of emails consume valuable computer resources but if the saved messages refer to individuals then they are also likely to be governed by the Data Protection Act 1998. This means that the subject of the message may have the right to request access to the email. Increasingly law courts are also asking organisations to compile data held in the form of emails as evidence in tribunals and other court cases. Emails should therefore not be retained for longer than is absolutely necessary.

As a rule of thumb, emails should be deleted after 6 months unless it is necessary to retain them for longer.

Further guidance on the retention of documents is available from the Federation’s IT Officer or House Bursar. The IT Officer can also advise you on good housekeeping practices regarding the storing and deleting of emails.

<table>
<thead>
<tr>
<th>Version control information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date last updated:</td>
</tr>
<tr>
<td>Date of next review:</td>
</tr>
<tr>
<td>Document owner / point of contact:</td>
</tr>
<tr>
<td>Last amended by:</td>
</tr>
<tr>
<td>Version number:</td>
</tr>
<tr>
<td>Status:</td>
</tr>
</tbody>
</table>

Appendix I: Key disposal/retention considerations criteria checklist

1. Has the document/record set been appraised?

As a first step, the nature/contents of any documents or records being considered for disposal should be ascertained. No document(s) should be earmarked or designated for disposal unless this has been done. Insofar as existing documents or records are concerned it follows that the above can only be achieved by inspection. The process may only take a few moments.

Nonetheless it can be a skilled task - depending on the complexity of the document(s) concerned –
and should only be undertaken by staff who possess sufficient operational knowledge to enable them to identify the document concerned and its function within the Federation. Any decision to the effect that future documents of a specified description be disposed of on expiry of a specified retention period should be an informed one i.e. taken with a full appreciation and understanding of the nature and function of the document/records.

The above is largely common sense, and hardly needs to be stated. However, if appraisal is inadvertently overlooked or carried out negligently, or by an employee who lacks the necessary background operational knowledge, the Federation runs the risk of important documents being destroyed in error.

2. **Is retention required to fulfil statutory or other regulatory requirements?**

There is very little specific legislation that stipulates mandatory retention periods for documents held by the Federation. However, staff should seek advice if they believe that there may be legislation which, either directly or indirectly, imposes minimum retention periods on the documents they are handling. For instance, minimum retention periods for certain financial records may be applicable.

3. **Is retention required to evidence events in the case of dispute?**

On rare occasions, the Federation may become involved in disputes with third parties. Such disputes, if not satisfactorily resolved, can result in reputational damage and the dissatisfied party potentially bringing legal proceedings against the Federation. Conversely, the Federation may wish to institute legal proceedings against an individual or organisation, e.g. to recover an unpaid debt, or in respect of faulty workmanship.

Where a dispute arises, or litigation has been commenced it is important that the Federation has access to all correspondence and other documentation that is relevant to the matter.

The Limitations Act 1980 specifies time limits for commencing litigation. The starting point therefore, is that the retention period is the length of time that has to elapse before a claim is barred. The majority of potential legal claims are statute barred on the expiry of 6 years. For this reason many organisations consider it prudent to retain files/records for a period of 6 years form the date when the subject matter was completed.

It is important, though, to keep in mind that in the course of the Federation everyday business large masses of document action are generated that serve no purpose after relatively short periods of time. Many documents will relate to completed matters where, realistically, the risk of subsequent litigation or other dispute is minimal, if not non-existent. Long-term retention of such documents is counter-productive. Staff should be prepared to carry out a risk analysis, with a view to disposal of such documents within a shorter period than the 6 years’ time frame.

4. **Is retention required to meet the operational needs of the Federation?**

In some cases retention may be desirable (whether permanent or otherwise) even though no minimum retention period applies or has expired. Staff should be aware of the risk of discarding documents or records that might be useful for future reference purposes (e.g. training), as precedents, or for performance management (performance indicators, benchmarking and comparison exercises). A professional judgement needs to be made as to the usefulness of a particular document.

5. **Is retention required because the document or record is of historic interest or intrinsic value?**
In most cases this consideration will not be applicable. However, it is possible that some documents/records may be of historic interest.

Where it is suspected that the document falls within this description appropriate enquires should always be made before taking any further action. The Director of IT or the Director of Business Management should be contacted for advice and guidance in the first instance.

Even if the document is of historical or monetary value, disposal rather than retention by the Federation, may well be the appropriate option (e.g. by way of transfer to a third party).
### Appendix II: Suggested retention period for different types of documents

<table>
<thead>
<tr>
<th>Type of record</th>
<th>Suggested retention period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accident records</td>
<td>3 years after end of investigation</td>
</tr>
<tr>
<td>Any information private to any individual</td>
<td>Destroy when no longer required</td>
</tr>
<tr>
<td>Bank records</td>
<td>7 years</td>
</tr>
<tr>
<td>Company records</td>
<td>Permanent</td>
</tr>
<tr>
<td>CVs and job applications not hired</td>
<td>6 months after notification</td>
</tr>
<tr>
<td>Disciplinary records</td>
<td>5 years following end of employment</td>
</tr>
<tr>
<td>Employer’s liability insurance certificate</td>
<td>40 years</td>
</tr>
<tr>
<td>General email correspondence</td>
<td>6 months unless likely that it will be need to retained for longer</td>
</tr>
<tr>
<td>Historical records relating to the Federation</td>
<td>Permanent</td>
</tr>
<tr>
<td>Medical and safety records</td>
<td>7 years</td>
</tr>
<tr>
<td>Personnel files</td>
<td>5 years following end of employment</td>
</tr>
<tr>
<td>Property records, trust deeds</td>
<td>Permanent</td>
</tr>
<tr>
<td>Redundancy records</td>
<td>6 years after redundancy</td>
</tr>
<tr>
<td>Sickness/sick pay records</td>
<td>3 years</td>
</tr>
<tr>
<td>Software and hardware inventory details</td>
<td>7 years</td>
</tr>
<tr>
<td>Tax records - self-employed or partnership</td>
<td>5 years from last tax date</td>
</tr>
<tr>
<td>Tax records - companies</td>
<td>6 years from last accounting period</td>
</tr>
</tbody>
</table>