## University of Warwick Data Retention Policy 2010

### 1. Introduction

The University of Warwick holds a great deal of important information that is crucial to the running of the organisation. While many information systems can be recovered after an incident the business critical data that resides in electronic and paper form must be suitably protected. This involves considerations into the confidentiality, integrity and availability (CIA) of business critical and potentially sensitive data.

The Policy is designed to the ISO 27001 standard and updated from BS 7799. Subsequently this policy shall be reviewed and updated regularly to ensure that it remains appropriate in the light of any changes to legal, contractual or acceptable use obligations.

### 2. Objectives

The objective of the Data Retention Policy is to provide guidance on the retention of the various types of data the University holds. This document strives to balance the need to store information with legal obligations to destroy the data safely when it is no longer required.

---

### Date | Version | Author | Comments
--- | --- | --- | ---
10/2007 | D01 | Clayton Jones | Guidelines on data retention, reviewed and amended by IPSC and Daryl Hindmarsh, ITS Director
10/2008 | D02 | Duncan Woodhouse | Consolidation of email retention policy, data retention guidelines and PCI DSS Policy
11/2008 | D03 | Duncan Woodhouse | Review and comments by Senior Assistant Registrar
01/2009 | D04 | Duncan Woodhouse | Review and comments by Deputy Registrar
06/2009 | F01 | Duncan Woodhouse | Ratified by Steering Committee
11/2009 | D01 | Duncan Woodhouse | Updates from the University Human Resource department and further consultation for 2010
3. Scope

The Data Retention Policy applies to information in all its forms. It may be on paper, stored electronically or held on film, microfiche or other media. It includes text, pictures, audio and video. It covers information transmitted by post, by electronic means and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

The policy applies to all staff and students of the University and to other users associated with the University. With regard to electronic systems, it applies to use of University owned facilities and privately/externally owned\(^1\) systems when connected to the University network directly or indirectly.

The policy applies to all University owned/licensed data and software, be they loaded on University or privately/externally owned systems, and to all data and software provided to the University by sponsors or external agencies.

4. Policy Statement

The University is committed to protecting the security of data through the preservation of

- **Confidentiality**: protecting information from unauthorised access and disclosure.

- **Integrity**: safeguarding the accuracy and completeness of information and processing methods.

- **Availability**: ensuring that information and associated services are available to authorised users when required.

The University will develop, implement and maintain the Data Retention Policy to ensure data is sufficiently stored, processed, transmitted and destroyed in a way consistent with our legal, contractual and ethical obligations.

4.1 Guidance on data retention

The University has developed a guide on how long certain types of data are retained. Please refer to the Appendix.

4.2 Considerations under the Data Protection Act

All University members will collect, retain and transmit personal data under the terms of the Data Protection Act 1998.

\(^1\) ‘Owned’ is deemed to include leased, rented or on-loan
The Act governs the collection, retention and transmission of information about living individuals and the rights those individuals have to see this information. The Act was updated in 2000 to cover personal data in both electronic and manual form.

**The principles are that personal data shall be:**

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept longer than is necessary
6. Processed in accordance with the data subjects rights
7. Secure
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

Personal data is defined by the Information Commissioner as any information about an individual from whom you are collecting, the compromise, loss or theft of which could cause distress or harm to that individual.

**Examples of personal data include:**

- Address
- Date of birth
- National Insurance Number
- Telephone numbers
- Benefit details
- Bank account details
- Information relating to the persons health or disability

For further information please see:

[http://www2.warwick.ac.uk/services/gov/legalservices/whentouse/dataprotection](http://www2.warwick.ac.uk/services/gov/legalservices/whentouse/dataprotection)

### 4.3 Considerations under Payment Card Industry Data Security Standards (PCI DSS)

All members of Warwick University must store, process and transmit payment card information in accordance with PCI DSS mandatory requirements. This standard applies to information held on paper as well as electronically and to transactions processed both online and via a third party terminal.

The University of Warwick processes payment card information, for donations, services, tuition fees and other areas. Therefore we are subject to the mandatory requirements of the Payment Card Industry Data Security Standards (PCI DSS) introduced in June 2007.

PCI DSS was created by the major credit card companies to improve consumer data protection. The main implication is that any risk from malicious activity, such as fraud and hacking, has been transferred to merchants (such as Warwick University) from the credit card companies.
Subsequently it is everyone’s responsibility to ensure payment card data is stored and used in the right way as any incident involving loss in confidentiality or integrity of this information could have a serious impact on the day-to-day operations of the University, its income, and its reputation.

The standard sets out 12 requirements that must be met in order to process credit or debit card information. Please read the following link for more information:

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Requirement 3 and 4 are of particular importance to Warwick University as they state we should:

- Keep cardholder data storage to a minimum
- Develop a data retention and disposal policy
- Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes
- NEVER store the card verification code or value or PIN verification value data elements.
- As a minimum render the Personal Account Number (PAN) unreadable anywhere it is stored
- Encrypt transmission of cardholder data across open, public networks (such as the main campus LAN)

Guidance on payment card information

For online transactions (such as WorldPay):

- University departments must only use a Finance Department approved supplier of online card payment services
- Payment card information should not be stored or processed on University servers
- Payment card information should not be transmitted across the campus network unless this is done securely

For third party terminal transactions (such as Streamline):

- University departments must only use a Finance Department approved supplier of terminal card payment services
- Payment card information must not be stored either on paper or electronically once a payment has been authorised
- The 3 digit security code must be completely erased following authorisation or ideally not kept at all
- Only the last four digits of the card number can be retained following authorisation
- Paper forms with any remaining card details recorded must be kept securely in locked cupboards with access limited to authorised personnel
- These paper forms must be destroyed as soon as they are not needed

Where information systems (including paper and electronic data) store payment information locally they must conform to PCI DSS standards. This may require an audit from an external, Qualified Security Assessor (QSA) and/or the completion of a Self Assessment Questionnaire (SAQ) as part of the ongoing risk assessment programme.

2 Locally refers to any desktop or server machine that resides on the local area network and/or has a Warwick IP address attributable to the University.
4.4 Disposal of Information

University members have an obligation to dispose of personal, confidential and business critical information in a secure manner.

For confidential paper information, members should ideally cross shred onsite and additionally put into the confidential waste steam.

For confidential, electronic information:

- DVDs/CDs should be shredded and then put into the recycling stream
- Computer hard drives and external storage media (such as USB sticks) should be wiped with a suitable software tool. No unencrypted data should be left on these types of media before re-using/recycling/disposal
- Media that cannot be wiped initially will need to be sufficiently protected before being overwritten e.g. storage tapes in a locked safe

5. Legal and Contractual Requirements

The University will abide by all UK legislation and relevant legislation of the European Community related to the holding and processing of information. This includes the following Acts and mandatory requirements:

- Copyright Designs and Patents Act 1988
- Data Protection Act 1998
- Freedom of Information Act 2000
- Payment Card Industry Data Security Standards 2007

The University will also comply with all contractual requirements related to the holding and processing of information.

6. Responsibilities

The Information Policy and Strategy Committee is responsible for the Data Retention Policy.

The University has established a strategic information security, risk management and business continuity function within the Deputy Registrar’s Office.

Heads of Departments, with support from the Deputy Registrar’s Office, are responsible for ensuring that information used within their department is managed and used in accordance with the Data Retention Policy.

All University members are responsible for protecting business critical and potentially sensitive data.

Everyone granted access to University information systems has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the Data Retention Policy.
All staff, students and other users should report immediately any observed or suspected breach of this policy to the Head of Department, the owner of the information, or, where the IT infrastructure is involved, IT Services Help Desk.

Those responsible for information or information systems, for example database and IT systems administrators, must ensure that appropriate security arrangements are established and maintained.

7. Policy Awareness and Disciplinary Procedures

The Data Retention Policy will be made available to all staff and students via the web as part of the Governance site, maintained by the Deputy Registrar’s Office, dedicated to the explanation and promotion of the policy. Staff, students, authorised third parties and contractors given access to the University information systems will be advised of the existence of the relevant policies, codes of conduct and guidelines.

Failure to comply with the Information Security Policy may lead to suspension or withdrawal of an individual’s access to information systems.

Members of staff

Failure of a member of staff to comply with the Information Security Policy may lead to the instigation of the relevant disciplinary procedures as specified in their terms and conditions of employment and, in certain circumstances, legal action may be taken.

Student members

Failure of a student to comply with the Information Security Policy may lead to the instigation of the disciplinary procedures specified in Regulation 23, and, in certain circumstances, legal action may be taken.

Minor infringements, such as causing inconvenience to other users, may lead to disciplinary action under the Minor Offences Procedure (Regulation 23 Subsection 6 and 7).

Major infringements, such as major breach of confidentiality, harassment, or illegal activities may lead to action under the Major Offences Procedure (Regulation 23 Subsections 8 and 9). This is not an exhaustive list of possible offences and the University will determine whether a case is minor or major having regard to all the circumstances of each incident.

---

3 Further information on the University’s staff disciplinary procedure is available on: http://www2.warwick.ac.uk/services/humanresources/newpolicies/disciplinary/

4 Further information on the University’s student disciplinary procedure is available on: http://www2.warwick.ac.uk/services/gov/calendar/section2/regulations/disciplinary
University contractors

Departments should have Service Level Agreements with contractors to ensure liability also rests with the contractor (sometimes called a Warwick agent) who is storing, processing or transmitting data obtained from the University.

Failure of a contractor to comply could lead to the cancellation of a contract and, in certain circumstances, legal action may be taken.

8. Information Security Education and Training

The University recognises the need for all staff, students and other users of University systems to be aware of information security threats and concerns, and to be equipped to support University security policy in the course of their normal work. Appropriate training or information on security matters will be provided for users and departments will supplement this to meet their particular requirements. The Deputy Registrar’s Office will undertake a proactive campaign of awareness and monitor/report upon the type and frequency of incidents.

9. Maintenance

The Data Retention Policy will be monitored by Information Policy and Strategy Committee and reviewed as necessary. Revisions will be subject to appropriate consultation.

The Deputy Registrar’s Office will report on a summary and exception basis, will notify issues and bring forward recommendations.

Heads of Departments are required to carry out periodic risk assessments and establish and maintain effective contingency plans. They are also required to carry out regular assessment of the security arrangements for their information systems.

Those responsible for information or information systems must carry out periodic risk assessments of their information and the security controls in place. They must take into account changes in business requirements, changes in technology and any changes in the relevant legislation and revise their security arrangements accordingly.

10. Related Policies

- Strategic information security is covered by the Information Security Policy on the Governance website.

- Use of University computing facilities is covered by Regulation 31 - Regulations governing the use of University Computing Facilities on the Governance website.

- The University has a separate Regulation of Investigatory Powers Act Statement [http://www2.warwick.ac.uk/services/gov/informationsecurity/policies/]
• Incidents related to bullying and harassment are covered in the Dignity at Work and Study Policy
http://www2.warwick.ac.uk/services/humanresources/newpolicies/dignity
# Appendix

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Retention Period</th>
<th>Reason for Length of Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel files including training records and notes of disciplinary and grievance hearings</td>
<td>5 years from the end of employment</td>
<td>References and potential litigation.</td>
</tr>
<tr>
<td>Application forms/interview notes</td>
<td>At least 6 months from the date of the job advertisement</td>
<td>Time limits on litigation</td>
</tr>
<tr>
<td>Facts relating to redundancies where less than 20 redundancies</td>
<td>6 years from the date of redundancy</td>
<td>As above</td>
</tr>
<tr>
<td>Facts relating to redundancies where 20 or more redundancies</td>
<td>12 years from the date of the redundancies</td>
<td>Limitation Act 1980</td>
</tr>
<tr>
<td>Income Tax and NI Returns, including correspondence with tax office</td>
<td>At least 3 years after the end of the tax year to which the records related</td>
<td>Income Tax (Employment) Regulations 1993</td>
</tr>
<tr>
<td>Statutory Maternity and adoption Pay records and calculations</td>
<td>3 years after the end of the tax year in which the maternity period ends</td>
<td>Statutory Maternity Pay (General) Regulations 1986</td>
</tr>
<tr>
<td>Statutory Sick Pay records and calculations</td>
<td>3 years after the end of the tax year to which they relate</td>
<td>Statutory Sick Pay (General) Regulations 1982</td>
</tr>
<tr>
<td>Wages and salary records</td>
<td>6 years</td>
<td>Taxes Management Act 1970</td>
</tr>
<tr>
<td>Individual pension entitlement and contribution history</td>
<td>As long as there is a member or dependant liability</td>
<td></td>
</tr>
<tr>
<td>Accident books, and records and reports of accidents</td>
<td>6 years after the date of the last entry</td>
<td>Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985</td>
</tr>
<tr>
<td>Health Records</td>
<td>During employment</td>
<td>Management of Health and Safety at Work Regulations</td>
</tr>
<tr>
<td>Health Records where reason for termination of employment is connected with health, including stress related illness</td>
<td>3 years</td>
<td>Limitation period for personal injury claims</td>
</tr>
<tr>
<td>Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999</td>
<td>40 years</td>
<td>Control of Substances Hazardous to Health Regulations 1999</td>
</tr>
<tr>
<td>Ionising Radiation Records</td>
<td>At least 50 years after last entry</td>
<td>Ionising Radiations Regulations 1985</td>
</tr>
</tbody>
</table>
### Student records, including academic achievements and conduct

<table>
<thead>
<tr>
<th>Duration</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>At least 6 years from the date that the student leaves the institution, in case of litigation for negligence.</td>
<td>Limitation period for negligence.</td>
</tr>
<tr>
<td>2 years from graduation for Exam scripts.</td>
<td>Reasonable period to cater for student enquiries which may need reference to examination scripts.</td>
</tr>
<tr>
<td>At least 10 years for personal and academic references.</td>
<td>Permits institution to provide references for a reasonable length of time.</td>
</tr>
<tr>
<td>Certain personal data may be held in perpetuity.</td>
<td>While personal and academic references may become ‘stale’, some data e.g. transcripts of student marks may be required throughout the student’s future career. Upon the death of the data subject, data relating to him/her ceases to be personal data.</td>
</tr>
</tbody>
</table>