Digital Records and Legal Admissibility: Explanatory Guidance

For whom is this guidance intended?

1. This guidance is for University staff with responsibility for ensuring that the appropriate legal weight is assigned to the digital records they create. It is of particular relevance to staff who:
   a. Need to maximise the legal weight of their records for statutory or regulatory reasons;
   b. Are responsible for information in corporate databases;
   c. Need to improve or update their current digital filing systems or databases.

2. This guidance provides a high-level overview of our current understanding of the law and details the best practice requirements.

What are digital records?

3. Digital records are records stored in digital format. There are two main types:
   a. Records "born" or created digitally, for example word processor documents, e-mails, spreadsheets or database records;
   b. Paper records copied to digital media, for example documents scanned into a digital filing system.

What is legal admissibility?

4. Legal admissibility concerns whether a court of law would accept a piece of evidence (in this case a digital record). Some evidence might be admitted to the court (i.e. is legally admissible) but the opposing lawyer might call the evidential weight into question. It would therefore be important for the University to prove that:
   1. The record is accurate, i.e. it is a complete and unaltered representation of the information;
   2. The record is authentic, i.e. that it is what it purports to be;
   3. The records has not been tampered with;
   4. The record is stored in a system that has been secure throughout the record's lifetime.

   If you cannot prove such factors, it will reduce the evidential weight of the record and could harm the case.

5. There are no firm rules for determining whether a digital record is legally admissible but it is possible to maximise its evidential weight by following this guidance.

Why might legal admissibility be a problem?

6. Digital records raise particular issues because:
   a. It is possible to make additions or deletions not apparent to the viewer of the document;
   b. It can be difficult to tell the difference between the original record and copies of it, which may have been altered;

c. Digital records are becoming highly sophisticated. For example a record could be made up of a word-processed document with a dynamic link to a spreadsheet. The record is then automatically updated when the spreadsheet is updated;
d. Digital records are often built temporarily and never recorded anywhere. Because systems can now source information from multiple systems, the information presented by them can be transient and consist of nothing more than temporary web pages built in response to a user accessing the system. It can be difficult to recreate the digital record or prove which information the user saw.

Why does the legal admissibility of digital records matter?

7. If the University's records are not legally admissible, they cannot be used to protect you or the University in court. This could result in expense and malicious litigation.

8. Maximising the legal weight of the University's digital records will also:
   a. Improve confidence in the reliability and authenticity of our digital records;
   b. Provide confidence to external regulators and auditors that evidence is authentic and accurate.

Who is responsible for ensuring that our digital records are legally admissible?

9. Business units are responsible for ensuring that their records are managed properly, which includes making provisions to safeguard the legal admissibility of digital records if necessary. In some cases, this means working with other units to ensure your records comply. For example, this applies to information held on a corporate database 'owned' by one unit, given IT support by a second unit, and gathered from a number of other units.

10. Legal admissibility is very rigorous and it would be a misuse of resources for all of the University's digital records to comply with this standard. Some records are more likely to be needed in the event of a dispute. You must decide which records those are. For example, many of the emails you receive will be ephemeral and have no long term value, whilst others will be important records perhaps recording authorisation to go ahead with a particular plan.

11. Undertake a risk assessment of your digital records. Consider the possible implications of being unable to demonstrate their evidential weight, balanced against the cost of implementing legal admissibility measures.

    Use the explanation and matrix below to help you make these decisions.

	High	Medium	Low	Very Low
1. What is the likelihood that your records will need to be legally admissible?				
2. How serious would the consequences be if your records were not legally admissible?				
3. How expensive will it be to keep the records at a legally admissible standard?				

Question 1. The legal admissibility of the University's records is not just about the University's ability to prove a case in court. The University may have to settle out of court because it lacks the legally admissible records to support its case.
Question 2. The consequences of being unable to demonstrate the authenticity of a record will depend upon a number of factors including the purpose of the record. Consequences of low evidential weight are greater for records that are required for regulatory compliance.
Question 3. The cost of maintaining records in compliance with legal admissibility standards will vary depending on your current IT system. Some systems require more work to bring them into compliance than others.

If your answer to the first question is High and your answer to the second question is High or Medium, ensure that records are maintained in accordance with PD 0008. If your answers to the first and second questions are Low or Very Low and your answer to the third question is High or Medium it is not worth maintaining records to the standards demanded by legal admissibility standards.

What are the main principles behind evidential weight?

12. If you are able to demonstrate the authenticity and accuracy of your records then they will have evidential weight. There are two main elements to demonstrating the authenticity of your digital records:
    a. "Freeze" records.
    b. Maintain documented audit trails.

13. "Freezing" means that from a specific moment in time, your system will not permit further changes to the contents of record. By doing this you can demonstrate that there were no changes to the file since it was "frozen" and you can prove the document's authenticity. If other versions or copies of the file develop, such as a revision to the word-processed document, these should also be "frozen" at defined times. You can then distinguish the "original" file from other copies and versions.

14. An audit trail provides supporting information and an historical record about the records being stored. It is similar to quality control measures and ensures you can demonstrate the authenticity of records. The audit trail should include:
    a. The name of the author of the information /document /database record;
    b. The date the record was stored;
    c. The names of people who accessed or made changes to the document;

d. Details of changes made to the record; version information;
e. Details of the record's movement from medium to medium, and from format to format;
f. The authentication measures used when the file is moved;
g. Evidence of controlled operation of the system where the record is stored;
h. Record access to the audit trail in the audit trail itself.

Follow documented procedures when accessing and interpreting audit trail data.

How do I maximise the evidential weight of our digital records?

15. The British Standards Institute (BSI) issued a code of practice on legal admissibility (DISC PD 0008:2004), Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Digitally, ISBN 0 580 42774 9). Compliance with the Code does not guarantee legal admissibility but will enable you to demonstrate that you are following best practices.

16. If after reading this guidance you decide to implement the requirements of the Code, refer to the Code itself for full details. If you decide not to implement PD 0008 you still need to follow best practice records management procedures for your digital documents. This includes taking account of issues such as version control ('freezing') and audit trails.

17. The following table outlines the requirements needed to maximise the evidential weight of your digital records. Refer to the code for further details.

What help is available?

18. The University Records Management Section provides advice, guidance and training on data protection, records management and freedom of information issues. Although we cannot set up individual procedures for you, we can provide training, facilitate workshops to help you comply with the Code, give you detailed advice on work in progress and serve as expert advisers on records management project boards.

19. Your IT support service can advise on the technical aspects of implementing legal admissibility requirements.

20. The Information Services Group (ISG) provide help and advice on facilities within ISG supported systems and software. They can help you to implement the guidance contained within this document. The Audit and Security Section of ISG provides advice on data security and related issues.

21. The Special Collections Department within the Library provides advice on digital preservation issues.

22. *DISC PD 0008:2004 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Digitally (ISBN 0 580 42774 9)* is published by the British Standards Institution.

Alexandra Dazey & Anne Gryzbowski
September 2009

	Requirements
1. Comply with the University's Framework	• Ensure records are managed in accordance with the University's Records Management Framework: http://www.recordsmanagement.ed.ac.uk/InfoStaff/rmstaff/RM_framework.htm. • You should also develop your own more detailed procedures. The Records Management Section has produced a series of guidance sheets to assist you: http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/records_management_for_staff.htm. • The Records Management Framework in combination with your own procedures will demonstrate to a court of law the normal business procedures for records management at the University.
2. Develop a retention schedule	• A retention schedule sets out how long you need to keep records. It will differentiate between important records and ephemeral records. • Developing a retention schedule helps you to decide the lifespan of your records. It means you will have proof that records are kept and destroyed in line with proper procedures. High profile cases (e.g. Enron) have highlighted the need to have proper policies for record destruction. • For more information please see the guidance notes on developing a retention schedule, http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/Retention/Retention.htm.
3. Create a procedure manual	• Create and maintain a procedure manual. Describe all procedures related to the operation and use of your system including input, output and operation. Provide staff with appropriate training to adhere to its requirements. Up to date documentation for procedures and processes will enable the University to provide evidence of normal working practice. • Document any changes to operational procedures in the manual and check that you do not compromise the requirements of the Code. Courts are less likely to question records managed in accordance with these practices. Keep superseded versions of the procedures manual for as long as you keep the records referring to them.

	• Establish policies and procedures as necessary covering the following: a. Responsibilities b. Maintenance c. Data capture d. Security and protection e. Authentication of records f. Data file transmission g. Data verification h. Indexing and scanning i. Long-term preservation j. Backup and system recovery k. System maintenance l. Use of contracted services m. Workflow n. Self-modifying files o. Date and time stamps p. Overlays, templates and presentation formats q. Voice, audio and video data r. Version control s. Encryption t. compression
4. Freeze and reconstitute data files	• Freeze relevant and important records to ensure their authenticity, eg. compound data files. • If you use compound data files, use audit trails to record the historical content of the data file. • It is important that you can reconstruct your records for a future date and time.
5. Maintain your audit trail	• Ensure that you collect and maintain sufficient audit trail information to track the movement and development of your records. • The audit trails should: a. If possible, be generated automatically by the digital system; b. Have an accurate associated date and time; c. Be available for inspection by authorised external personnel who have little or no familiarity with the digital system; d. Be kept securely to prevent any change to the data; e. Not be modifiable. • When preparing information for evidence you must provide supporting information (an audit trail) to demonstrate that your records are authentic. The audit trail provides an historical record of the stored records and the system.
6. Comply with IT Security Policy	• Ensure your records comply with the IT Security Policy produced by the Audit and Security Section of the ISG and approved by University Court. See: http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/security-policies/security-policy

	• The Audit and Security Section monitor and analyse the methods and techniques of external attack on the University and its IT infrastructure. Consult someone with knowledge of the digital system you are using to assess any particular risks. • Develop procedures to prevent modifications to stored information going undetected. The digital system must be able to detect any modifications made to records (especially unauthorised modifications), and that a record of modifications can be produced to the satisfaction of a court of law. • It is important that all risks to the security of your digital system are identified and minimised. Security violations might involve: a. Unauthorised access to or disclosure of information; b. Unauthorised communication with or use of computing equipment;; c. Enabling unauthorised access to computing equipment and IT systems d. Distributing information that may encourage or lead others to attempt unauthorised access to computing equipment and IT systems; e. Damaging, contaminating, destroying, erasing or undermining data contained on computer equipment, including the introduction of computer viruses; f. Fraudulently obtaining a financial or other advantage or causing detriment to another through manipulation of data.
6. **Set and document access permissions**	• Document the levels of access available in the digital system. • Only permit staff with relevant access rights to create new records or edit existing ones. In court you must be able to prove who had access to the digital records and what level of access they had.
7. **Ensure data accuracy and data authenticity**	• Confirm that facilities within the digital system are adequate to ensure the ongoing preservation of data accuracy and authenticity, including during the transfer of data to and from the storage media and protection from malicious software (for example viruses). • Ensure individuals checking data are different from individuals inputting data. This provides a check on errors and deliberate falsification of records.
8. **Document system procedures and**	• Consult your IT support service to create and maintain system documentation and procedures, such as a system portfolio and change control register. • Ensure documentation provides a description of how your system operates.

operations	Include information about: a. Your system's hardware and software; b. Network elements that comprise your digital system and how they interact. c. Document media handling and storage procedures. • The manual should provide users with details of the system at any given time in its period of use. This includes the specification of your system, the type of network you are using, any software patches you have applied and when you applied them. • The system documentation and procedures will help to demonstrate the normal operations of your system and show that your records have been kept normally. • You should also maintain: a. A maintenance log, detailing the maintenance to your digital system, and b. A quality control log, detailing quality control checks to your digital system.
9. **Document special techniques**	• Document any special techniques you use, such as compression. If lossy compression is used, compare a sample set of decompressed files with the originals to check there is no significant loss of information. Lossy techniques remove information from data files during the compression process and when decompressed the file may not be identical to the original. Record where this is the case.
10. **Ensure long-term preservation**	• Ensure that you make provision for long-term access to files. The Library can advise on digital preservation issues and solutions. See: http://www.lib.ed.ac.uk/digpres/. • Storage media (such as CDs, floppy disks or backup tapes) have a finite life. Stored information must be retrievable. Check media periodically in accordance with manufacturer's recommendations.
11. **Comply with hardware recommendations**	• Ensure that you adhere to hardware manufacturer's recommendations for the operational environment of the system. • Consider environmental factors such as temperature stability, humidity management, safeguards against power fluctuations and protection from physical threats.
13. **Assess compliance with the Code**	• Undertake periodic audits of your digital system to ensure it is working properly and that you adhere to the requirements of the Code. Keep records of the audit until you have completed two further audits, i.e. keep the records of the two most recent audits.