Digital Records and Legal Admissibility: A Summary

For whom is this guidance intended?

1. This guidance is intended for University staff responsible for ensuring that the appropriate legal weight is assigned to digital records. It is of particular relevance to staff that need to maximise the legal weight of their records for statutory or regulatory reasons, are responsible for information in corporate databases or need to improve or update their current digital filing systems or databases.

What is legal admissibility?

2. Legal admissibility concerns whether a piece of evidence (in this case a digital record) would be accepted by a court of law. If a record does not hold evidential weight, it could potentially harm a case being fought.
3. Some of your records will have more potential significance to a court of law than others and therefore need to hold more evidential weight. You must decide which records these are by undertaking a risk assessment of your digital records. Consider the possible implications of being unable to demonstrate their evidential weight.

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

4. 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.

What are the main principles behind evidential weight?

5. If you are able to demonstrate the authenticity and accuracy of your records then they will have evidential weight. There are two main elements that demonstrate authenticity of digital records:
   a. Your system's ability to "freeze" a record at a specific moment in time;
   b. Maintenance of a documented audit trail.

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

6. 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 Electronically (ISBN 0 580 42774 9)).* Compliance with the Code does not guarantee legal admissibility but it does define best practice and will enable the University to demonstrate that it complies with the approved and documented normal working practices.
7. For more information, consult the key points on the following page of this document. For a more detailed explanation, please see our explanatory guidance. http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/LegalAdmiss/legaladmiss.htm

What help is available?

8. The University Records Management Section provides advice, guidance and training on records management and information compliance issues. Your IT support service can advise on the technical aspects of implementing legal admissibility requirements. The Audit and Security Section of Information Services Group (ISG) provides advice on data security and related issues. The Special Collections Department within the Library provides advice on digital preservation issues.

Maximising the evidential weight of digital records: key points

- Ensure that you manage your records in accordance with the University's **Records Management Framework.** 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

- Compile a **retention schedule** for your records. A retention schedule will differentiate between important records and ephemeral records.

- Create and maintain a **procedures manual**. Describe all procedures related to the operation and the use of your system including input, output and operation.

- **Freeze relevant and important records** to ensure their authenticity. Freezing means that from a specific moment in time, your system will not permit further changes to the contents of record.

- Maintain an **audit trail**. The digital system must contain a secure record of all read-write accesses to the data. Audit trails should enable you to assess the historical content of the data file whenever necessary.

- Develop, authorise and implement an Information Security Policy. Manage your records in accordance with the University's Information Security Policy.

- Set and document **access permissions** available to the digital system. Only permit staff with relevant access rights to create new records or edit existing ones.

- Confirm that facilities within the digital system are adequate to ensure that **data accuracy and data authenticity** are preserved throughout the lifetime of your records.

- Document **system procedures and operations** to show how the system operates and to demonstrate that it was operating correctly.

- Document any **special techniques** you use, such as compression.

- Plan for the **long term preservation** of your records so that you can read and retrieve them for as long as they are needed.

- Ensure that you adhere to the **hardware manufacturer's recommendations** for the operational environment of the system.

- **Audit** compliance with the Code periodically to demonstrate that you are meeting its requirements.

Alexandra Dazey
September 2009