Digital Information – Lifecycle Management (DILM) – Key Considerations

Background

1. The following five page guidance document explains the rationale for why each of the 10 questions have been included in the Digital Information Lifecycle Management – Key Considerations form in support of both the University's information compliance obligations and its ongoing institutional resilience (e.g. through digital continuity).

2. The General Data Protection Regulation 2016 ('GDPR') requires the University to consider data protection and privacy issues 'by design' i.e. upfront and before any processing of data takes place. To meet this obligation the University needs to put in place the appropriate technical and organisational measures to ensure that it adheres to the six data protection principles and that it can safeguard the privacy rights of individuals.

3. The approach set out at paragraph 2 data protection by design and by default means the University needs to integrate or 'bake in' data protection into its processing activities and business practices, from the design stage right through the information lifecycle. In practical terms a digital information system that processes personal data would need to have functionality that allows for:

    - data to be exported in response to a Subject Access Request (SAR);
    - inaccurate data to be rectified;
    - identification of to which party personal data may have been disclosed;
    - erasure of specified personal data held within the system at the appropriate time (e.g. as a result of a right to erasure request or in line with the Record Retention Schedule;
    - a stop to be put on processing an individual's data either on a temporary basis or permanently where a successful 'right to object' has been lodged;
    - porting of personal data to another organisation (data controller) where this is "technically feasible".

N.B. The above list of potential digital Information system functionality to support data protection requirements is not exhaustive. The table at page 3-5 sets out fuller details.

4. Digital Information Systems that either process personal data or other information assets and that are not configured with functionality that supports the lifecycle management of information can expose the University to the following risks:

- Non-compliance with statutory or other regulatory requirements (e.g. health and safety, finance, research [and associated funding], data protection legislation, the Freedom of Information Act 2000 and other transparency legislation).

    - The result of noncompliance with Data Protection legislation can lead to harm and distress caused to data subjects in certain instances (e.g. a result of their personal data being divulged or accessed by a third party or where the University is not able to comply with a request by them to exercise their privacy rights e.g. to provide a copy of their data to them or to erase it) for which they may receive compensation. There is also the risk of reputational damage to the University and a fine of up to €20 million, or 4% of total worldwide annual turnover, whichever is higher.

    - The result of non-compliance with the Freedom of Information Act 2000 can lead to a decision notice- publicised on the ICO website - and the University compelled to comply with remedial actions prescribed to the University by the ICO.

- Poor decisions based on inaccurate or incomplete information;

- Financial or legal loss if information required as evidence is not available or cannot be relied upon;

- Possibility of unauthorised access, amendment or disposal of information;

- Failure to protect information that is vital to the continued functioning of the University, leading to inadequate business continuity planning;

- Unnecessary costs caused by storing records and other information for longer than they are needed;

- Staff time wasted searching for records and time wasted considering issues that have previously been addressed and resolved.

5. In each case the explanation for the inclusion of a question in the key consideration form that is set out in the table at pages 3-5 focuses on a few supporting examples (drawn mainly from statutory compliance obligations) and as such there will likely be other additional reasons to include each question in this form.

6. In addition each question promotes adherence to the six principles of the University's Information and Records Management policy (IRM) and good (ISO standards based) IRM practice. This approach also supports the University in circumstances when it is required to produce authoritative and trustworthy records (e.g. in legal proceedings). Further information is available through contacting: recordsmanagement@warwick.ac.uk

Information Lifecycle – Key Consideration	Why is this a Key Consideration
1. Can information be easily identified and searched for in the system?	This functionality in a Digital Information System supports adherence to: Purpose limitation principle of GDPR Data Minimisation principle of GDPR Accuracy Principle of GDPR Storage Limitation Principle of GDPR Right of access (GDPR) Right to data portability (GDPR) Right to erasure (GDPR) Right to Rectification (GDPR) Accessibility of digital information for as long as it is needed (Digital Continuity).
2. Can information imported into the system continue to be accessible in its original format (e.g. Word, Excel, PDF)	This functionality in a Digital Information System supports adherence to: Freedom of Information Act 2000 (Section 46) Accessibility of digital information for as long as it is needed (Digital Continuity).
3. Are there controls to protect information from unauthorised access, alteration, deletion and use?	This functionality in a Digital Information System supports adherence to: Accuracy Principle of GDPR Integrity and Confidentiality principle (GDPR) Right to Rectification (GDPR) Right to restrict processing (GDPR) Accessibility of digital information for as long as it is needed (Digital Continuity).
4. Is it possible to access earlier versions of information held in the system?	This functionality in a Digital Information System supports adherence to: Data Minimisation principle of GDPR Accuracy Principle of GDPR Right to Rectification (GDPR)

Information Lifecycle – Key Consideration	Why is this Key Consideration
5. Can audit reports be produced that record actions taken on information held in the system (e.g. audit report captures: imports, exports, downloads, versioning, internal and external access, sharing and deletions etc.)?	This functionality in a Digital Information System supports adherence to: Integrity and Confidentiality principle (GDPR) Freedom of Information Act 2000 (Section 46) Freedom of Information Act and Environmental Information Regulations – Retention and Destruction of Requested Information
6. Is information capable of being exported (a) individually (b) in bulk in a format that would allow its continued usability (e.g. identification and access) outside of the system?	This functionality in a Digital Information System supports adherence to: Freedom of Information Act 2000 (Section 11) – Means by which communication to be made Environmental Information Regulations 2004 (Section 6) – Form and format of information Right of access (GDPR) Right to data portability (GDPR) Accessibility of digital information for as long as it is needed (Digital Continuity).
7. Can the system be automated to carry out the deletion of information in line with agreed time periods (e.g. those set out in the University Records Retention Schedule (RRS)? *	This functionality in a Digital Information System supports adherence to: Storage Limitation Principle of GDPR Accuracy Principle of GDPR Right to erasure (GDPR)
8. Is there functionality for information that relates to identified or identifiable living individuals (personal data) to be anonymised or destroyed after a designated period of time in line with the relevant entry in the University's RRS? *	This functionality in a Digital Information System supports adherence to: Storage Limitation Principle of GDPR Accuracy Principle of GDPR Right to erasure (GDPR) Freedom of Information Act and Environmental Information Regulations – Retention and Destruction of Requested Information

Information Lifecycle – Key Consideration	Why is this Key Consideration
9. Will destruction of information selected by authorised users result in its obliteration or inaccessibility so that it cannot be restored through operating system features or specialist data recovery techniques? *	This functionality in a Digital Information System supports adherence to: Storage Limitation Principle of GDPR Accuracy Principle of GDPR Right to erasure (GDPR) Freedom of Information Act and Environmental Information Regulations – Retention and Destruction of Requested Information
10. Can the system provide confirmation of information that has been destroyed and when (e.g. a system generated report that includes metadata necessary to identify the information and its time and date of destruction)?	This functionality in a Digital Information System supports adherence to: Storage Limitation Principle of GDPR Accuracy Principle of GDPR Right to erasure Freedom of Information Act and Environmental Information Regulations – Retention and Destruction of Requested Information

The following standards have been drawn upon to develop the questions set out in the key considerations form:

- BS ISO 15489-1:2016 - Information and documentation — Records management
- ISO 16175 (Parts 1-3) - Information and documentation — Principles and functional requirements for records in electronic office environments
- BS ISO 23081-1:2017 - Information and documentation — Records management processes — Metadata for records
- BS 10008:2014 - Evidential weight and legal admissibility of electronic information – Specification
- ICO Guidance - Deleting personal data - 20140226 Version: 1.1