EDINBURGH NAPIER UNIVERSITY

GOVERNANCE SERVICES

Guidance on the Safe Disposal of Confidential Waste

Purpose of this Guidance

As it is essential for the effective administration of the University that redundant or time expired information is destroyed routinely, all employees need to know when records can be disposed of and the most appropriate method(s) for doing this. Data Protection Legislation (UK GDPR and DPA 2018), the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Regulations 2004 (EIRs) impose specific requirements for the timely and secure disposal of paper and electronic information.

Scope

This Guidance is informed by the above statutory requirements and applies to all staff, including temporary and associate staff, all employed or visiting students and contractors.

1. Retention of Records

1.1 Data Protection Legislation requires that information is held only for as long as necessary, whilst under FOISA and the EIRs it is an offence to dispose of certain records before a prescribed period has elapsed. These prescribed periods are often dictated by other legislation and regulations. In order to meet our statutory obligations, the University has developed Records Retention Schedules for staff guidance (please contact dataprotection@napier.ac.uk for access). Initial guidance is given in s.20 of the Data Protection Code of Practice which includes links to JISC's Business Classification Scheme and Records Retention Schedules for Further and Higher Education Institutions.

1.2 Governance Services also publishes guidance on Records Disposal and the Use of Consoles, which gives advice on records that can be routinely destroyed and what constitutes a confidential record.

2. Destruction of Records

University records should be destroyed in accordance with your area's records retention schedule and/or after seeking advice from the Information Governance team. Once you are satisfied that you may dispose of records which you hold, particularly where you have primary responsibility for a set of records (see the definition of a 'Golden Record'), it is recommended under FOISA that you create a log of those records which you have destroyed. You can do this by using the template record disposal form on which you should include:

- a brief description of the record
- the appropriate justification for disposal e.g. current academic year + one
- the date it was done; and
- the method used e.g. disposal in a confidential waste console bin.

3. Disposal of Paper Material

This includes **all** manual records e.g. printed documents, handwritten and post-it notes.

3.1 Routine paper waste i.e. blank forms, early drafts of non-sensitive work, publicity material and 'junk' mail should be put in the office paper recycling bin. If you have large quantities of white paper material which do not contain any personal data or confidential or commercially sensitive information and you think this may be recyclable, please contact your Cleaning Supervisor for advice on how to dispose of it.

3.2 Any records containing personal and sensitive personal data (Data Protection CoP definitions section) about staff, students or third parties **must** be disposed of in a confidential waste console bin.

Particular care must be taken with:

- any material that contains sensitive personal data i.e. health issues, racial or ethnic origin, political opinions or trade union membership, religious or similar beliefs or criminal convictions
- other significant personal data that refers e.g. to staff or student performance measures or grievance or complaint matters

3.3 Any records containing confidential or commercially sensitive information about University business, particularly where an exemption to the disclosure of this information under FOISA has been applied, **must** also be placed in a confidential waste console bin.

3.4 If you work from home either on an occasional or regular basis, you must **not** dispose of any paper records which contain personal or sensitive data or confidential or commercially sensitive information, in your domestic waste. All such paper records **must** be returned to the University and disposed of in accordance with this guidance.

4. Disposal of electronic material and hardware

4.1 Electronic records held on your work computer should be deleted in accordance with 1.1 and 1.2 above and/or on advice from the Information Governance team. You should also check the deleted items folder on 'Outlook' and the 'Recycle Bin' on your desktop to ensure they have both been emptied.

4.2 Physical electronic devices and CDs, DVDs and memory sticks which contain the types of records referred to in 3.2 and 3.3 above **must** also be securely disposed of in accordance with this Guidance.

4.2.1 Blackberrys, Tablets and other PDAs must be reformatted or permanently wiped. The IS Service Desk should be contacted on ext. 3000 for guidance on how to dispose of

other University owned electronic devices and the personal and/or confidential data which they contain.

4.2.2 CDs, DVDs and memory sticks must be disposed of in dedicated console bins provided at each campus. The Property & Facilities Helpdesk on ext. 5000 will be able to advise where these bins are located.

4.3 The University has a process for the disposal of redundant hardware to ensure that this is done securely. The Redundant Equipment Notification form should be completed, authorised and emailed to Procurement in Finance Services.

4.4 In accordance with guidance issued by Information Services, when working from home University staff are required to use secure remote access to records containing personal data and should not copy such records to a home PC. University staff must also consider the security implications of the disposal of home computers which may have any University records retained on their hard drives. Where necessary, advice on disposal should be sought from the IS Service Desk.

5. Sanctions for data protection breaches

Failure to dispose of records in accordance with this Guidance may result in disciplinary action being taken where appropriate and access rights to personal data being suspended or removed. In addition, the UK Information Commissioner has the power to impose monetary penalties up to a maximum of £17M / 4% annual global turnover on the University where a serious data breach has occurred, or to take enforcement action.

6. Advice and Guidance

Please contact the Information Governance team for data protection and records management advice at:

: dataprotection@napier.ac.uk