EDINBURGH NAPIER UNIVERSITY

MANUAL AND PHYSICAL DATA SECURITY POLICY

Introduction

In order to meet the requirements of the UK Data Protection Legislation (GDPR and DPA 2018), the University is obliged to have in place a framework designed to ensure the security of all personal data during the collection to destruction cycle.

Scope of the Policy

This policy relates only to the retention and storage of personal data held in hard copy, such as on paper or on physical devices e.g. laptops, external drives, USBs (memory stick or flash drive), DVDs, CDs, tablets and smartphones, etc. The retention and use of electronic data is covered separately by the University's Information Security Policy and its subsidiary policies, further information and guidance on which is available from Information Services.

This policy applies to all University employees, including associate, temporary and casual staff members.

The University provides a secure electronic network with IS approved systems and expects that processing of personal data will take place within the University network using approved systems the majority of the time. However, it is recognised that there are exceptional circumstances where this is not possible and in these cases it may be necessary to use processing systems referred to in this Policy. Please note that these should be the exception and the University's secure electronic network should be used primarily and routinely. Some historical records may be retained in physical format until such time as they reach the end of their retention period.

1. Keeping Personal Information Secure

1.1 All personal data, whether in hard copy or stored on a physical device must be kept in a secure environment with controlled access. The level of security applied should be agreed after a basic risk assessment has been carried out as provided for at 3. below. Appropriate secure environments include:

- locked metal cabinets with access to keys limited to authorised personnel only
- locked drawer in a desk (or other storage area) with access to keys limited to authorised personnel only
- locked room accessed by key or coded door lock where access to keys and/or codes is limited to authorised personnel only

1.2 All staff must receive appropriate, specific induction in their area, on manual data security requirements.

1.3 Where access to personal data is required on a frequent basis e.g. historical data, and therefore maintaining locked drawers or cabinets at all times is impractical, then steps must be taken to ensure authorised personnel are in attendance at all times when the storage facility is unlocked.

1.4 Files containing personal data must never be left unattended while removed from their normal locked storage area. Staff must therefore adopt a clear desk policy, in relation to files and documents containing personal information, at all times when they are out of their offices or away from their work area.

1.5 Where applicable, staff should consider whether records which require to be kept for longer than two years should be removed to the University's off-site storage facility.

2. Access to Personal Data

2.1 Managers must designate the individual members of staff who by nature of the post, have been identified as requiring legitimate access to personal data in the course of their employment.

2.2 In addition, the designated purposes for which access to personal data will be permitted must also be defined. For some departments this will be clear in relation to the function of the department or service e.g. Student Support Services or Human Resources. However, in other cases this will require to be specifically defined.

2.3 From time to time all staff will have access to personal data about other members of staff or students and confidentiality must be observed by all staff at all times. When temporary staff are employed in posts which involve access to, and processing of, personal data, confidentiality agreements should be included within the Terms and Conditions of Employment and a separate Oath of Confidentiality should be signed.

2.4 Where a file containing personal data is removed in response to a legitimate request by another authorised member of staff, this must be subject to a strict signing out and return procedure, which is the responsibility of the person holding the file.

2.5 The Manager of the relevant area will be expected to designate a member of staff with responsibility for overseeing departmental arrangements for the removal and return of records.

2.6 The occasions when personal information is photocopied should be kept to a minimum. Where this is necessary, the provider of the information is responsible for ensuring all copies are returned once the task in question has been completed and subsequently disposed of in accordance with the guidance note referred to in section 5.2 below.

2.7 Where staff are required to take manual personal data home with them, appropriate security precautions must be taken to guard against theft, loss or inappropriate access. This will include securing data in a locked briefcase, never leaving data unattended in a public place and ensuring that all reasonable precautions are taken to secure data at home and whilst in transit. Avoid taking hard copy personal data off University campuses wherever possible.

In accordance with guidance issued by Information Services, when working from home University staff are required to use University managed laptops or secure remote access (as provided by the University) to electronic records containing

personal data and should not copy such records to a home PC or personal mobile device.

2.8 Staff should ensure that visitors for whom they are responsible are signed in and out at the relevant campus reception desk and are accompanied in areas normally restricted to staff.

3. Risk Assessment

3.1 A risk assessment will require to be carried out as appropriate by the Deans of Schools or Directors of Service or by an individual designated by them.

3.2 The purpose of the assessment is to establish the potential risks for unauthorised access to personal data and to define appropriate actions to eliminate or at least mitigate the risk, of unauthorised access.

3.3 The appropriate Managers will be expected to consult the University's Information Security Classification Scheme in taking all reasonable steps to address any potential risks identified.

4. Third Parties

4.1 Institutional arrangements must ensure the security of all personal data which may be transferred to, or processed by, a third party.

4.2 In advance of any external transfer of personal data, University staff are required to consider whether such a transfer is authorised under any relevant data sharing agreement, or is otherwise required by, or permitted under the Data Protection legislation. The purpose, fairness and transparency of any transfer must always be considered and staff must ensure that they have consulted the University's Data Protection Code of Practice at Section 8: Data Sharing, prior to any such external data sharing.

4.3 Where external data sharing has been considered necessary or is permitted under 4.2 above, the appropriate security precautions should be taken to minimise the risks of loss of data and/or accidental third party disclosure.

4.4 All communications should be marked strictly private and confidential and addressed to a named individual.

4.5 Physical devices containing personal data e.g. USB memory sticks, CDs, DVDs, must always be encrypted before being removed from University premises. Removal of such portable physical devices containing personal data must be with appropriate permission of your line manager. The sensitivity of the information must be considered and if the risk of harm to individuals, in the event that the device is lost/stolen, are high then it is not appropriate to remove the device from University premises.

4.6 The most appropriate secure method of sending the information must be considered i.e. by hand delivery, registered or recorded delivery as advised by the University's Mail Room or by use of a courier, double enveloped or securely packed, as necessary given the number of pages being sent.

5. Disposal of Personal Data

5.1 All data will be retained only for the designated periods in the University's Records Retention Schedules. The Information Governance team will provide further advice and guidance on request.

5.2 All personal data must be disposed of securely and safely in accordance with the University's guidance on Safe Disposal of Confidential Waste.

6. Security Incidents

6.1 All incidents where the security of personal data has been compromised or where there have been any suspected security weaknesses or threats must be reported immediately by the relevant Dean of School or Director of Service in which the breach has occurred and to the Information Governance team (dataprotection@napier.ac.uk) in accordance with the Procedure for a Breach of Data Security .

6.2 The Data Protection Officer and/or the Information Governance Manager will decide in the particular circumstances of the breach whether it is serious enough to inform the University Secretary and will liaise as appropriate with any other key staff.

6.3 Any breach of security policies and procedures by a member of staff or student will be dealt with through the relevant formal disciplinary processes, where necessary.

7. Disaster Recovery

7.1 Vital records are records which, in the event of a disaster, are essential to maintain business continuity by continuing or resuming operations, recreating an institution's legal and financial status and preserving the institution's rights and fulfilling its obligations to its stakeholders. (JISC)

7.2 Appropriate arrangements must be made for manual records which are classed as 'vital records', including fire-proof storage, off-site storage and backing up in electronic form e.g. by scanning. However, as electronic copies of such records will not provide the same evidential weight as the original document, the Manager with responsibility for such records must consider which arrangements are appropriate and seek advice as necessary from Governance Services.

7.3 Each Dean of School or Director of Service must ensure that the vital records register held within their area's Business Continuity Plan is regularly reviewed and updated as required.

8. Responsibilities for the Application of this Policy

8.1 The University Leadership Team (ULT), via Deans of Schools and Directors of Service, is responsible for ensuring the requirements of this policy are implemented. Compliance with the requirements of this policy may be the subject of random audits by Governance Services or the University's Internal Auditor.

8.2 All University employees are responsible for ensuring compliance with this policy and any other related University policies or guidance.

9. Further Information

Staff are advised to download the checklist on Security of Personal Information and retain this for reference purposes. Anyone requiring further information or guidance on any aspect of this policy or on the undertaking of risk assessments should contact the Information Governance team (dataprotection@napier.ac.uk).

Title	Manual and Physical Data Security Policy
Author	Governance Services
Date first Approved	February 2012
Review Date	February 2015
Reviewed by	University Information Governance Group
Approved by	Risk, Resilience & Audit Monitoring Committee
Last Approval date	June 2019
Next review date	May 2023
Minor review date	Jan 2025
Scope	All University employees, including associate, temporary and casual staff members.