University of the Highlands and Islands

Information Security

Data Protection Policy

Contents

SECTION 1 3

UHI Control

1.1 UHI Reference 3
1.2 UHI Author and Version Control 3
1.3 UHI Policy Summary 4

SECTION 2 5

Introduction

2.1 Purpose 5
2.2 Scope 5
2.3 Compliance 5
2.4 Terminology 5

SECTION 3 6

Policy

3.1 Policy Statements 6
3.2 Responsibilities 6
3.3 Review period 7

Revision history

Rev	Date	Description	Author	Review	Check	Approve
0 Draft A	22/03/11	First draft for comment.	D. Jarvis	IW	MY	JIL
0 Draft B	26/05/11	Incorporate feedback following workshop	D. Jarvis	IW	MY	SP
0 Draft C	07/06/11	Incorporate changes post workshop discussion	D Jarvis	IW	MY	JAL
0	08/07/11	Final Candidate Rev 0 release	I. Whittaker			JAL
1	17/08/11	Final version for FGPC	J Cribb			

SECTION 1

UHI Control

1.1 UHI Reference

Policy reference	UHI IS DP
Responsible committee and officer	FGPC

1.2 UHI Author and Version Control

Original author:	Douglas Jarvis (Amor Group)
Current revision author: (if applicable)	Julie Cribb

Version Control

Version	Date	Author	Purpose/change	Policy review date
01	17/08/11	J Cribb	For FGPC	30/08/11
02				
03				

UHI Approval

Version	Date approved	Approving committee	Individuals/groups to be notified (if relevant)	Committee officer signature
01	30/08/11	FGPC		
02				
03				
04				

Prior to implementation, **approval** is required from Finance and General Purposes Committee or Court.

1.3 UHI Policy Summary

Overview **Why is the policy required?**	This Staff Policy is part of the ISO/IEC 27001:2005 policy documentation set.
Purpose **What will it achieve?**	This policy sets out UHI's commitment to protecting personal data and complying with relevant legislation and describes how that commitment is implemented.
Scope **Who does it apply to?**	It applies to all personnel whether staff, contractor, other third parties, or members of partnership organisations with access to UHI data or information systems.
Consultation/notification **Highlight plans/dates**	
Implementation and monitoring **(including costs)**	
Enforcement **Detail how the policy will be enforced and who will be responsible**	
References **(highlight any advice received from external organisations)**	

SECTION 2

Introduction

2.1 Purpose

The University of the Highlands and Islands (UHI) has educational and business requirements to maintain certain personal data about living individuals in pursuit of its legitimate activities as a university. UHI recognises that the correct and lawful treatment of personal data maintains confidence in the organisation and provides for successful operations.

Personal information, whether held on paper, on computer or other media, is subject to the legal safeguards specified in the Data Protection Act 1998.

UHI fully endorses and adheres to the eight principles of the Data Protection Act 1998. These principles specify the legal conditions to be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Employees, students and any others who obtain, handle, process, transport and store personal data for UHI shall adhere to these principles.

2.2 Scope

This policy applies to all personnel who, during the course of their normal duties, will have access to the information processing systems operated by UHI and its partnership organisations and to all data whether stored electronically on systems, applications or paper copy.

2.3 Compliance

This policy applies to all staff, contractors and third parties who are given access to information systems by UHI and its partner organisations. The data protection processes defined in this document are mandatory. Since the policy underwrites legislation, legal proceedings as well as disciplinary action are likely to be taken against UHI staff and contractors who fail to comply with this policy.

2.4 Terminology

The word "**shall**" is used throughout this document to state where a policy is a mandatory requirement.

The word "**should**" is used throughout this document to state where a policy is a recommended requirement.

For the purposes of this policy the term "**personnel**" includes both UHI and partnership organisation staff, contractors, students and third parties who have access to Information Systems.

SECTION 3

Policy

3.1 Policy Statements

UHI shall:

- Maintain an up to date and accurate register entry with the Information Commissioner's Office (ICO);
- Ensure that any changes are notified to the ICO within appropriate timescales;
- Ensure that there is someone with specific responsibility for Data Protection;
- Observe fully the conditions regarding the fair collection and use of personal data;
- Meet its obligations to specify the purposes for which personal data is used;
- Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- Ensure the quality of personal data used;
- Apply strict checks to determine the length of time personal data is held;
- Ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act;
- Take the appropriate technical and organisational security measures to safeguard personal data;
- Ensure that appropriate safeguards are in place for personal information being transferred outside the UK. Note: Additional safeguards are required when the information is being sent outside the EU;
- Ensure that the rights of people, about whom information is held, can be fully exercised under the Act (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information);
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

3.2 Responsibilities

Line Managers shall ensure that all staff and contractors are adequately briefed and comply with this policy.

Information Owners shall ensure that, where appropriate:

- documents containing personal information have appropriate classification applied (See UHI's Information Classification Policy);

- retention polices are applied to personal information held on file (See UHI's Information Retention Policy).

The **Data Protection Officer** shall be responsible for setting out clear data protection procedures including responding to requests for information.

Personnel responsible for managing and handling personal information shall follow good data protection practice and comply with this policy.

3.3 Review period

This policy shall be reviewed and updated if appropriate after a period of twelve months.