UNIVERSITY OF ABERDEEN

POLICY FOR ACCESS TO PERSONAL DATA

Policy for dealing with either external or internal requests to the University for access to personal and sensitive personal data in terms of the Data Protection Act 1998, as affected by the Regulation of Investigatory Powers Act 2000 and other related legislation.

(METADATA)

Version 0.2: 1 September 2010
Version 0.3: 2 March 2011
Version 0.4: 23 May 2011

APPROVALS	**DATE**
AGIS	9 March 2011
UMG	
PNCC	X
COURT	CT10-11:47.6 Approved by Court 28.06.2011
Review by: PPG; DIT; HR; REGISTRY	2 years from X above

CONTENTS

1 SUMMARY AND REASONS FOR THIS POLICY

1.1 This Policy is necessary because, from time to time, enquiries are received, in particular by Human Resources, Registry and by the Directorate of Information Technology, from bodies inside and outside of the University for access to personal data of staff or students held by the University. There is a presumption under the Data Protection Act 1998 that the University, as Data Controller, will protect the confidentiality of personal data and will not release it. However, there are certain criteria which allow the release of personal data to the party requesting it.

1.2 On behalf of the University, as Data Controller, staff dealing with requests have to balance the privacy rights of the individuals under the European Convention on Human Rights, as applied to the UK by the Human Rights Act 1998, the Scotland Act 1998 and the Data Protection Act 1998, against the University's legal obligations to comply with lawful requests which are:

(i) Received from outside of the University and claiming rights under the Regulation of Investigatory Powers Act 2000, or the Regulation of Investigatory Powers (Scotland) Act 2000, eg for interception and monitoring of staff and/or student equipment; and/or

(ii) From outside or inside of the University for access to Personal and Sensitive Personal data.

The Data Subject may be absent or unable to give consent, or unaware of an ongoing confidential investigation being undertaken.

1.3 This Policy (1) sets out the procedural steps for ensuring that the criteria for allowing release of personal data are met by the staff of the University who hold such personal data, and (2) provides a trail for the authorisation of release of such data.

2 OBJECTIVE

This Policy also enables the University to ensure a common and consistent approach of delivery, and proportionality of response to requests for Personal and Sensitive Personal data.

In all instances, if the reader is in any doubt as to interpreting this Policy, they should contact the University Data Protection Officer or one of the decision-makers referred to in paragraph 5.3 of this document.

This Policy details the steps to be followed by staff who receive a request for access to personal data in order to comply with the Data Protection Act 1998 and the Human Rights Act 1998 regarding access to Personal and Sensitive Personal data.

This document is written to provide protection to both the Data Subject or that person's area being searched, and to the staff members asked to give access to the information when the owner of the information is absent. Thus ensuring a standard and consistent approach is used for taking decisions when any College, School or Support Service across all Service Desks, is asked to give access to personal data.

3 ABBREVIATIONS OF RESPONSIBLE PERSONNEL

HR Human Resources
DIT Directorate of Information Technology
PPG Policy, Planning and Governance
DPO Data Protection Officer
DC Data Controller (Court of the University of Aberdeen)

4 SCOPE

4.1 This Policy covers:

(i) Requests which are exceptional, ie supported by Police statutory or common law powers, or Court Warrant, or Government letter, eg from the UK Borders Agency; or Police Special Branch authorisation;

(ii) Requests to access HR files, hard copy or electronic, or e-files or emails on servers maintained by DIT.

This Policy is **NOT** intended to apply to:

(i) Business as usual or routine enquiries from the police or other public bodies;

(ii) Requests for access to shared discs accessed by a group of users, in which case the co-ordinator of the group will decide and, if in doubt, the group co-ordinator will refer the request to PPG;

(iii) Subject Access Requests (SARs) from Data Subjects about their own records. If the recipient of the request from a Data Subject is in doubt, the Data Subject should be referred to the DPA post box: dpa@abdn.ac.uk, or to the DPO.

Such routine enquiries may continue to be processed by the appropriate Support Service Desk or Service Centre Manager or Head of Service Delivery, under their own procedures but, if there is any doubt, the enquiry should be referred to PPG for clarification.

4.2 All requests processed under this Policy will be logged, tracked and resolved in a timely manner and recorded in an Exceptional Disclosure Log, to be maintained in PPG on behalf of the Data Controller.

4.3 All staff who receive requests for personal data are responsible for identifying requests as either (i) exceptional (for processing under this Policy); or (ii) business as usual for processing within their own Service Area.

If in doubt, a request should be referred to PPG/DPO/PPG secretaries (ext 2016 and ext 2093), or dpa@abdn.ac.uk.

5 PROCEDURES/MAIN STEPS FOR EXCEPTIONAL REQUESTS

5.1 All personal data access requests, which are exceptional, must be logged within PPG. This must include verbal requests and should be logged as they happen. It would be difficult for an audit to be conducted without the full written facts and the absence of such a log may put the University in a vulnerable position.

5.2 Once the request is logged by PPG, it will co-ordinate the decision-making for granting or refusing the access request.

5.3 A decision will be taken by not less than three out of the 12 postholders listed below of whom one will be from DIT:

3	Director of DIT plus two Deputy Directors of DIT
2	Director of HR plus another
2	Director of PPG plus DPO
1	Senior Vice-Principal
3	Vice-Principals (not otherwise involved with the Data Subject)
1	University Secretary
12	

5.4 Any of the postholders, if unable to pass the responsibility on in their temporary absence to one of their other named postholders, may nominate in writing a temporary custodian who would act on his/her behalf.

5.5 If the access request is granted:

- PPG to contact the requisitioner and request the subject matter to be searched for and an appropriate save date of the data to be accessed.

- PPG to confirm that it is appropriate to proceed and this decision must be communicated in writing to DIT, HR or Registry, as appropriate, and to the requisitioner. This decision must be archived as part of the call log.

- If PPG indicates it is not appropriate to proceed, this decision must be communicated in writing to DIT, HR or Registry, as appropriate, and to the requisitioner. This decision must be archived as part of the call log.

- HR to arrange a convenient time for the line manager of the Data Subject (user) in question, HR representative and DIT representative to meet for accessing the private files.

- Files, folders or email that appear marked as personal must not be accessed unless there is a decision specifically taken by the three postholder decision-makers after taking into account all circumstances and (i) the application of statutory exemptions, if any, and (ii) the presence of any external requests and their statutory powers of access.

- PPG to conclude the correspondence with the requisitioner.

6 RELATED DOCUMENTS

Policy Zone: University Policies

http://www.abdn.ac.uk/hr/policies/information-security.shtml

http://abdn.ac.uk/dataprotection/

http://www.abdn.ac.uk/dit/documents/cond-IT.pdf (Conditions for using DIT Facilities).

Title	Policy For Access To Personal Data
Author / Creator	David Blair, Data Protection Officer
Owner	Data Protection Officer
Date published / approved	Court approved June 2011
Version	1
Date for Next Review	Reviewed: 1st June 2015 Next Review : June 2016 (annual review)
Audience	All Staff and Students
Related	Policy on Data Protection
Subject / Description	Policy for dealing with either external or internal requests to the University for access to personal and sensitive personal data in terms of the Data Protection Act 1998, as affected by the Regulation of Investigatory Powers Act 2000 and other related legislation
Equality Impact Assessment	-
Section	Policy, Planning and Governance
Theme	Governance and Compliance
Keywords	PPG, Staff, Students, Data, Protection, sensitive, legal,