University of St Andrews

Requests for personal data by the Police or a similar third party for the purposes of the prevention or detection of crime, apprehension or prosecution of offenders, or for taxation

Document type	**Policy**
Scope (applies to)	All staff
Applicability date	18/06/2019
Review / Expiry date	18/06/2024
Approved date	01/07/2019
Approver	Vice-Principal
Document owner	Head of Info Assurance & Governance
School / unit	Office of the Principal
Document status	Published
Information classification	Public
Equality impact assessment	27/04/2012
Key terms	Information governance and management/Data protection/Sharing personal data with third parties
Purpose	To provide controls so that personal data are lawfully released to the Police and other authorities for the purposes of crime prevention and detection or taxation purposes

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
2.1	Policy reapproved following periodic review – minor changes made following changes to data protection law (2018)	Approved	C Milne	19 June 2019

The University of St Andrews is a charity registered in Scotland, No: SC013532

1. Introduction

This Policy establishes the conditions under which personal and/or sensitive personal data ("personal data") for which the University has responsibility as a Controller under the Data Protection Act 2018 ("the DPA" or "the Act") will be released for the purposes of crime or taxation, as defined by the DPA.

1.1. Where the policy applies

The Policy applies to all requests made by the Police, or other authorised agencies for personal data held by the University, where the requestor seeks that information for the purposes of ***the prevention or detection of crime or for taxation,*** and where it is not appropriate for the requestor to seek that information from the individual(s) concerned.

This Policy is not concerned with the release of information to the Police or other persons in an emergency, e.g. details of medical conditions, next of kin etc.

1.2. Policy statement

It is the University's policy that the transfer of personal data (in all forms) a third party for the purposes of carrying out their statutory functions in relation to the prevention or detection of crime, the apprehension or prosecution of offenders or for taxation will not take place unless the conditions set out within the DPA and guidance as to the interpretation of the relevant provisions of the Act from the Courts or the UK Information Commissioner can be met.

1.3. Policy objectives

This Policy seeks to ensure that, in relation to the management of requests for the release of personal data by the University for the purposes of the prevention or detection of crime, or the apprehension or prosecution of offenders, or for taxation, that:

- Suitable controls exist to protect the rights and freedoms of individuals and to limit the University's exposure to any claim from an individual or from any penalty that a regulator could impose, arising from a breach of the DPA;
- Staff are provided with direction as to where requests for the release of personal data are to be passed;
- Those empowered to make decisions are clearly identified; and
- The steps to be followed in the decision making process are set out, and are made subject to regular review.

2. Release of personal data in relation to crime and taxation

The DPA provides the facility for the University (as a data controller) to release personal data to a third party, when conducting their statutory functions for the following purposes:

a) The prevention or detection of crime;
b) The apprehension or prosecution of an offender; or
c) The assessment or collection of any tax or duty or of any imposition of a similar nature.

Unless a Court order is made, the decision regarding whether to release personal data will belong to the University and the University alone.

2.1. Conditions for the release of personal information for the purposes of the prevention or detection crime or for taxation

The University will ***only*** consider release of personal data for the purposes of the prevention or detection of crime or of taxation (see section 2 above) where:

- Denying the information request would impede the requestor's ability to undertake a lawful duty, connected with the purposes of the prevention or detection crime or apprehension or prosecution of offenders or for taxation (see section 2 above); and
- The requesting body could not obtain the information requested from a source other than the University; and
- Release of the information would not conflict with other legal obligations with which the University is required to comply.

Or:

- Where a Court Order is made that requires the University to release the requested information.

2.2. Managing the release of personal information for the purposes of the prevention or detection of crime or for taxation

2.2.1. A valid request

In most circumstances a valid request will consist of the following:

i. It must normally be made in writing, or in another permanent recorded form.

- Requests made by telephone or in person (where no written request is provided) are not generally acceptable.

ii. A written request will normally be made using a standard Police form, which can include that approved by the Association of Chief Police Officers (ACPO) and the UK Information Commissioner. In any event, the information to be provided must normally include:

- A summary of the reason as to why the information is required and is not otherwise obtainable;
- Details identifying the individual(s) about whom personal data is being sought;
- The precise information required about the individual(s);
- The name, rank and number of both the requesting and authorising Police Officers;
- The signatures of both the requesting and the authorising Officer; and
- Subject to part iii below, the authorising Officer to be senior in rank to the requesting Officer and of a rank no lower than Inspector.

iii. Where the Police cannot provide sufficient details as to why they seek the information to support the purposes set out in section 2 of this Policy without prejudicing an investigation and/or operation, the request must be authorised by an Officer of the rank of ***Superintendent or above***.

iv. Where a request for personal data, for the purposes of crime and taxation is received from a Local Authority or another body, those persons tasked with assessing whether personal data are to be released for the purposes of crime and taxation (See this Policy, Section 2.2.2) shall determine

whether the request has been made with an equivalent level of detail and authorisation to that expected of the Police in similar circumstances.

2.2.2. Authorisation

Requests for the release of personal data to the Police or any other body for the purposes of the prevention or detection of crime or for taxation **must** be managed by one of the following, or in their absence a nominee:

- Vice-Principal, Governance;
- The Head of Information Assurance and Governance;
- The Proctor;
- The Director of Student Services;
- The Chief Legal Officer;
- The Academic-Registrar; or
- The University Security Manager.

The decision to release the requested information will be made against the criteria set out in this Policy. These mirror guidance issued by the UK Information Commissioner concerning section 29 of the DPA.

2.2.3. Action on receipt of an invalid request

Should a request be judged to be invalid by the University for one of the following reasons:

- Not made in writing (or another permanent form);
- Insufficient information to allow the University to determine whether the requested information can or should be released; or
- Not approved by the appropriate ranking Officers (which may require a Superintendent or greater, depending on circumstances)

then the request will be refused (normally in writing) and the requestor will be asked:

- To return with the required information and/or appropriate approvals; or
- To seek a Court order requiring the University to release the requested information.

2.2.4. Documentation of decisions

All requests to release information for the purposes of crime or taxation must be documented for audit purposes, such documentation to include a copy of the request, the initial assessment of the request and a summary of the actions taken by the University.

This information is to be held separately from the student or staff file, by the Information Assurance and Governance function, and access to this information will be restricted.

Records of requests will be retained for period of 24 months following the receipt of the request, after which they are to be irreversibly destroyed.

Release of information

Where the University decides that it is obliged to release personal (in any form), then it will release only the minimum information necessary for the requestor to conduct their lawful duties.

The University will not provide a third party with access to information systems enabling that party to search for information – unless compelled to do so by Court Order.

2.2.5. Acting with the knowledge that a request has been made for the purposes of the prevention or detection of crime or for taxation

Duty of care

By receiving a request for information for the purpose of the prevention or detection of crime, the apprehension or prosecution of offenders, or for taxation the University may become aware of events/circumstances where it may wish to act, so that it can address its duty of care and other responsibilities. The University will not act on any knowledge gained from the receipt of such an information request without first seeking guidance and, as necessary, permission from the requestor. Such communications between the University and the requestor will be documented for audit purposes.

Subject access requests

Where the University has legitimately released personal and/or sensitive personal data of an individual for the purposes of the prevention or detection of crime or for taxation, if an affected individual seeks information from the University concerning those actions (under the subject access right to information) then the University is not required to make a response (and will not respond), as that right is not available, where personal data are released, for the purposes as stated, above.

3. Responsibilities

3.1. Members of staff

Should a request for information by the Police or a similar authority be made, then that is to be referred to one of the post holders listed in this Policy, section 2.2.2.

Details of information requests made for the purposes of the prevention or detection of crime, apprehension or prosecution of offenders or for taxation are to be kept strictly confidential. Any form of further use of information surrounding such requests outwith the requirements of an individual's job role/description, or any instruction issued to them, may constitute a criminal offence and a breach of this and other University Policy.

3.2. Other responsibilities

The Vice-Principal, Governance will be responsible for the implementation of this Policy. The Head of Information Assurance and Governance will be responsible for advising on technical aspects of this Policy, including emerging guidance and for holding all documentation (see this Policy, section 2.2.4).

4. Implementation

Those University Officers referred to herein may appoint a nominee to exercise their duties as per this Policy as and when appropriate.

5. Methodology

This Policy was developed making reference to similar policies adopted by other UK higher education institutions and with reference to guidance issued by the Office of the UK Information Commissioner concerning the operation of the Data Protection Act 1998[1].

On conducting an equality impact assessment no equality or diversity issues were identified as likely to arise through this Policy's implementation.

6. Review

This Policy will be reviewed at regular intervals. That review period will be recorded on the accompanying coversheet for this Policy. Any significant change to relevant legislation, University Policy or procedures primarily concerned with information *confidentiality, integrity and accessibility* may trigger an earlier review. This Policy will be presented to the Principal's Office for approval.

7. Reporting breaches

In the first instance any suspicion of a breach of this Policy should be reported to the Head of Information Assurance and Governance.

8. Sanctions

Failure of a member of staff to comply with this Policy may result in disciplinary action being taken. Where it is believed that a criminal action has occurred, the University will report this to the Police. The University reserves the right to pursue civil damages against any party.

Where a serious breach of the DPA has occurred, namely where unwarranted and unauthorised access to personal information has occurred (in terms of volume or sensitivity) and where the potential harm to individuals has become an overriding consideration, then the University Head of Information Assurance and Governance and Data Protection Officer, will report the matter to the UK Information Commissioner.

9. Availability

This Policy will be published on the University web site and through the University Freedom of Information Publication scheme. This Policy can be made available in different formats, in which case please direct any requests to the University Service Desk (Information Services).

10. Contacts/further information

Enquiries regarding this Policy can in the first instance be directed to the Head of Information Assurance and Governance.

11. Document history

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
1.0	Approved version updated – reflecting feedback received from Principal's Office	Approved	C Milne	18-May-2012

[1] Information Commissioner's Office (2015), Using the crime and taxation exemptions: Data Protection Act. Available online: https://ico.org.uk/media/1594/section-29.pdf, Accessed 05-October-2016.

1.0	Approved Principal's Office			May 2012
1.1	Service Directors Group approved that the post holders listed in section 2.2.2 can provide a nominee to manage the release of personal data in their absence	Approved	C Milne	15-Aug-2012