**St Georges, University of London (SGUL)**

**Law Enforcement Personal Data Requests Policy**

1. **Scope**
   1. This policy applies to the one-off sharing of University personal data with the Police or other relevant government agencies such as HMRC, UKVI, DWP or local government authorities, for the purposes of law enforcement.
   2. This policy does not apply to routine, scheduled sharing of personal data, for which a data sharing agreement should be put in place.
   3. All requests for information falling within the scope of this policy must follow the strict rules outlined in this document.
2. **General**
   1. UK Data Protection Legislation includes exemptions that allow an organisation to choose to disclose data without being in breach of the Law, if it is persuaded that doing so is both necessary and proportionate for:

* the purpose of safeguarding national security or
* the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty
  1. Information should only be disclosed where the University is happy that one of the above conditions exists and where the University is in receipt of a valid request.
  2. The University is not obliged to respond to a request unless the request is accompanied by a warrant or there is a law which requires us to do so. Any legal requirement to disclose data can be verified with the University’s General Counsel.
  3. Before releasing any personal data to the Police or other agency, the University must satisfy itself that the request relates to a legitimate and properly authorised investigation.

1. **Roles and responsibilities**

3.1 The decision to release data can only be made by the following role holders:

* The Director of Human Resources (or designated deputy) or the Chief Operating Officer in the case of staff records
* The Academic Registrar (or designated deputy) or the Chief Operating Officer in the case of student records
* The Chief Operating Officer and the Student Union Chief Operating Officer in the case of Student Union records where the personal data originated from the University
  1. The Director of HR and the Academic Registrar will ensure that alternative arrangements are in place whilst they are away from the University, by assigning responsibility for dealing with requests to an appropriate member of staff in their absence.
  2. In the case of an unplanned absence of the Director of HR or Academic Registrar, requests should be escalated to the Chief Operating Officer to deal with.
  3. All requests to the University must:
* be submitted in writing (by post or by email) and on headed paper
* be submitted by a case officer from the relevant agency, or in the case of the Police be countersigned by a senior police officer
* specify who the request relates to and the exact categories of personal data they are requesting
* confirm why the requested data is necessary for their investigation
* where the request claims there is a law requiring us to disclose, they must provide details of that law and the specific part of that law relevant to their request
  1. When responding to requests the University staff member responsible for disclosing the data should ensure that:
* the data is shared securely using the appropriate University system, e.g. encrypted email or iDrop
* the data being shared is limited to what is absolutely necessary
* the disclosure is properly documented using the form in Appendix A
* the decision to disclose is confirmed with the Data Protection Officer to provide an audit trail
* the student or staff member whose information is being shared has been notified unless this would compromise the investigations of the relevant agency (this should be confirmed with the agency requesting the personal data)

3.5 Untrammelled access to personal data by the Police will only be provided by the University on the production of a search warrant. In such cases the decision to reveal the contents of any individual’s entire mail box will be taken by the Principal alone (or designated Deputy in her absence).

1. **Controls**

4.1 The Data Protection Officer will be responsible for any necessary updates to this document with regard to changes in the law.

4.2 Ownership of the policy will sit with the Information Governance Steering Group. The IGSG will include the policy in the schedule for the review of information governance policies and procedures.

# Appendix A

**St Georges, University of London (SGUL)**

**Record of Personal Data Disclosure**

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| This form should be completed and sent to the Data Protection Officer as record of the disclosure. You do not need to name the individual student(s) or staff whose personal data has been shared, or give a detailed description of the data shared, on this form. But you should make sure you keep a full record of the disclosure, including a copy of the information disclosed and the requester’s paperwork, in line with the University’s records retention schedule. | | | |
| Name of person disclosing data: |  | | |
| Job Title: |  | | |
| Email address: |  | Telephone: |  |

|  |  |
| --- | --- |
| Name of organisation requesting data: |  |
| Job title of person submitting request: |  |
| Valid paperwork received (Yes/No): |  |

|  |  |
| --- | --- |
| Personal data requested: |  |
| What law enforcement purpose(s) is the data being requested for?: | *Safeguarding national security, prevention/detection of crime, apprehension/prosecution of offenders, assessment/collection of tax/duty* |
|  |
| Why is this personal data necessary for the requester’s investigation?: |  |

|  |  |
| --- | --- |
| Reason(s) for decision to disclose: | *Include details of any legal requirement placed on the University to disclose this data, e.g. a specific law or provision of a warrant* |
|  |
| Has the relevant student or staff member been informed (Yes/No)?: |  |
| If they have not been informed what was the reason for this?: |  |

|  |  |
| --- | --- |
| How was the data provided to  the requester?: | *Encrypted email, password-protected encrypted file, secure uploads server (iDrop)* |
|  |
| Date information was disclosed: |  |
| Signed: |  |