GUIDELINES ON DISCLOSURE OF STUDENT, GRADUATE AND EMPLOYEE INFORMATION

Table of Contents

1. Introduction and purpose

The purpose of this guidance is to ensure that personal data and/or confidential information about individuals is managed in accordance with our privacy notices and that information is disclosed internally or to third parties only under appropriate circumstances, with approval of all such requests by the Data Protection Officer or their delegate. It applies to non-routine disclosures (i.e. not those covered in relevant privacy notices) and where the consent of the subject has not been obtained.

Imperial receives requests for release of information contained within its student, graduate and employee records from various third parties, which can include:

- Individuals (e.g. family members of a graduate, recognised teaching centre personnel)
- Media organisations (e.g. for data regarding a public figure)
- Employers (e.g. for verification of information about job applicants)
- Other universities (e.g. for verification of qualifications of applicants)
- The police (where information is sought to assist with an investigation)
- Competent authorities (e.g. the Home Office and local authorities to assist with VISA, fraud and tax liability enquiries)
- Regulatory bodies (e.g. the General Medical Council)

Such requests can be received by any Imperial employee, but most commonly by the Student Records team (Registry), Security Services and the data protection team.

2. Overarching principle

Imperial will not disclose personal information other than as described in our privacy notices without the consent of the individual. The exceptions to this are:

- where a competent authority, or similar (as listed above), formally requests information for a legitimate purpose and such disclosure is permitted by data protection legislation.
- where to withhold such information could be detrimental to the student, to the interest of the public, and to the reputation and standards of the university.

3. Verification of student qualifications

GUIDELINES ON DISCLOSURE OF STUDENT, GRADUATE AND EMPLOYEE INFORMATION

Imperial College subscribes to the Higher Education Degree Datacheck (HEDD) online verification service for employers and agencies to verify the qualifications of students and alumni of the College. Enquirers wishing to verify student qualifications will be directed to use that service.

4. Requests about deceased students, graduates or employees

Information about a deceased person does not constitute personal data and is therefore not subject to data protection legislation. However, the data about deceased students, graduates or employees held by the University is subject to the Common Law Duty of Confidentiality. In addition, the records held may include data about other living individuals to which data protection legislation would apply.

The individual or organisation requesting data about a student, graduate, or employee who has died needs to provide:

- Independent evidence of the death of the a student, graduate, or employee. This can be a death certificate or trusted media source (e.g. an obituary or a news story).
- Evidence of relationship to the individual
- A statement on the purpose of their request for the data.

The data protection team will assess whether disclosure is appropriate on a case-by-case basis.

5. Wide-ranging police requests for information about victims

In most instances, police requests are for specific limited information, usually address and contact details. On occasion, the police ask for more extensive information about an individual who is a witness to or victim of a crime. In such cases, the subject's consent will be obtained and the request will be managed through the subject access procedure.

6. Requests for CCTV footage of accidents and incidents from third parties

Insurance companies and legal representatives may seek to obtain CCTV footage of road traffic accidents and other incidents that may have been captured by CCTV cameras managed by Imperial. The data protection will determine whether disclosure is justified and assess whether disclosure would involve the personal data of others in the relevant footage in line with Imperial's Data Protection Code of practice 4 – CCTV.

7. Internal disclosure requests with University Secretary approval

Imperial College London's policies and Codes of Practice permit access to system information, which may include the personal data of members of staff and students, in specific circumstances with the authorisation of the University Secretary. These include:

- In the event of a suspected or actual information security incident or an unacceptable network event, ICT may take action to examine any systems on the College network.
- Access to email accounts of staff who have left the College (or who are unable to consent) for continuity of business purposes.
- Access to email accounts or other network data for investigation of disciplinary matters
- Data on access to buildings for audit, compliance or investigation purposes.
- CCTV images for investigation of disciplinary matters or incidents
- Covert CCTV monitoring for investigation purposes (with approval of Head of Security and University Secretary)

8. Protocol for Managing Data Release Requests

The receiver of the request, if not the data protection team, will refer it to the data protection team (by emailing subjectaccess@imperial.ac.uk).

A member of the team will check that the disclosure is compliant with data protection legislation and College policies.

Competent authorities will usually have a form which is used to set out their powers to require information and/or to state the applicable exemption (these are set out in Schedule 2 Part 1 (2) of the Data Protection Act 2018). All police forces have such a form. If such a form would usually be provided, the data protection team will ask that the enquiry is resubmitted using the appropriate form.

Where the agency does not have an approved form, we will require the requester to state why they are asking for the information and for what purpose.

If the request is legitimate and it is determined that the information should be disclosed, the data protection team will request the information from the relevant department, review to ensure only relevant and necessary information is disclosed and disclose to the requester.

The data protection team will record the details of the request and whether the information was disclosed.