

Information Rights: Subject Access Request Procedure

Under data protection legislation, all staff, students and other users about whom we process personal data have rights associated with its use.

These rights are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

An individual may make a request relating to any of the rights listed above to Ravensbourne University London (“the University”). Data Subjects shall have the right to require us to correct or supplement erroneous, misleading, outdated or incomplete personal data. In order to exercise a particular right, a Data Subject must make what is known as a Subject Access Request.

All such requests will be considered by the University in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

How to make a Subject Access Request (SAR) to The University

Subject Access Requests should be made preferably by email to the Privacy Officer (dpo@rave.ac.uk) or in writing to following address:

Privacy Officer
Ravensbourne University London
6 Penrose Way
London
SE10 0EW

The person making the Subject Access Request should provide the following details:

- Full name;
- Date of birth;
- Course (for student or alumni) or department (for staff or former employees); - Student number or University employee number, if relevant or known; - Information would like to access such as:
 - (a) Student: Student record, grades, student support or disability records.
 - (b) Staff: HR records such as employment file, personal development discussions, safety records, etc.
- Location where the information is likely to be held, if known.
- Contact details i.e. email, address, phone number.

Any member of staff receiving a Subject Access Request should refer that request **immediately** to the Privacy Officer.

Verification of Request

The Privacy Officer will use appropriate means to verify that the requestor is the Data Subject or their authorised legal representative and may ask the requestor to provide proof of identity. If the request is being made by a Solicitor acting on your behalf they will be asked to provide written consent and a copy of your ID. The Privacy Officer will then confirm that the request is genuine with you.

Response

The Privacy Officer will provide a response to any request within 30 days of the receipt of the written request with proof of identity from a Data Subject. A request will be deemed received once all the relevant information has been provided by you and the validity of the request has been verified.

In the unusual circumstance that the Privacy Officer cannot respond fully to the request within 30 days, the Privacy Officer can take up to an extra 2 months to respond. The Privacy Officer will inform you within 1 month of the initial request and will explain why more time is needed. The Privacy Officer will also provide you or your authorised legal representative with the following:

- An acknowledgement of receipt of the request.
- Any information located to date.



- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the appropriate individual who the Data Subject should contact for follow up.

The information provided in response will normally be in electronic format. If you require the information in another format, you should ask the Privacy Officer if it is possible.

The University will provide the following additional information within its response:

- the purpose for processing this information;
- specific categories of personal data which is processed;
- confirm whether the data has been or will be disclosed to third parties and/or other Countries;
- confirm data is stored according to the retention schedule;
- individual rights applicable;
- information about the individual's right to complain to the Office of The Information commissioner; and
- confirm the existence of automated decision making, if relevant'

Internal Process

The Privacy Officer will identify and collate the information across the relevant internal departments and systems where it may be held. Depending on the specifics of Data Subject's Request, this may require comprehensive searching of relevant:

- databases;
- drives;
- emails;
- other structured or semi structured files; and/or
- unstructured files (if a particular piece of information is requested).

The Privacy Officer will liaise with relevant departments and IT to identify all places where the data is processed or held.

The Privacy Officer will screen the information in detail to ensure that it is liable for disclosure and that no other data subject's rights are infringed by disclosing it. This will be done on a case-by-case basis for each individual piece of information. In some cases only parts of particular documents will be disclosed and parts will be redacted to protect the privacy of others. For instance, if the record is primarily about the data subject, with incidental information about others, then that third party information will be redacted. If the record is primarily about third parties, with incidental information then it may be withheld if redacting or third party consent is not possible. Records which contain advice from University lawyers, contain requests for legal advice or were written as part of obtaining legal advice will not be disclosed. Information which would prejudice the prevention or detection of a crime will not be disclosed. For example, if the police informed us that a student is under investigation, but the student did not know this, then that information will not be provided to the student whilst the investigation is in progress. It will only be disclosed if the investigation is closed or if the student has been informed that there is an investigation.

Manifestly Unfounded or Excessive Requests?

Where a request is received that the Privacy Officer believes is manifestly unfounded or excessive, Ravensbourne may charge the data subject a fee or refuse to comply with the request. A request may be considered manifestly unfounded or excessive where amongst other things it merely repeats the substance of an earlier request. If the Privacy Officer declines a Subject Access Request or requests a fee, the Data Subject will be informed of the decision and:

- (a) the reasons for the request being declined;
- (b) the Data Subjects right to make a complaint to the Information Commissioner's Office; and
- (c) their ability to seek to enforce this right through a Judicial remedy.

Requests for Data Access by Third Parties

In certain circumstances prescribed by the law, Ravensbourne is permitted to disclose Personal Data to third parties such as the police, a local authority or other authorised agencies.

Examples of these circumstances include, but are not limited to where information is needed:

- for the prevention or detection of crime
- for Taxation
- for matters of National Security
- where it is not appropriate for the requestor to seek that information from the individual(s).

The University may also release of information to the Police or other persons in an emergency, e.g. details of medical conditions, next of kin etc.

Ravensbourne will comply with such requests when:

- 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 for taxation; and
- The requesting body could not obtain the information requested from a source other than the University; and
- Release of the information does not conflict with other legal obligations with which the University is required to comply

Only the minimum information necessary for the requestor to conduct their lawful duties will be released in such circumstances.

Such requests must normally be made in writing to the relevant department (HR in the case of staff (hr@rave.ac.uk) or Registry in the case of students (registry@rave.ac.uk) . Requests made in person and/or by phone must be verified to ensure that the requestor is bona fide and the request is valid.

The release of information must be authorised by an appropriate member of staff:

- Requests about students should be authorised by the Head of Registry (or in their absence the Director of Student Recruitment and Success or University Secretary and Chief Compliance Officer)
- Requests about staff should be authorised by the Director of HR (or in their absence the University Secretary and Chief Compliance Officer or Vice Chancellor).

For more information on Data Subject Rights, you can visit the Information Commissioner's Office Website: <https://ico.org.uk/>