Ravensbourne University London: Data Protection Policy

Owner:	Data Governance Board
Author	Craig Clark
Date	09/07/2021
Version	2.0
Document Security Level	PUBLIC
Review Date	07/09/2023

Ravensbourne University London

1. Introduction

1. Ravensbourne is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

2. This Policy outlines the roles and responsibilities of current employees, enrolled, prospective or former students and all Data Processors must comply with in order to comply with the law and ensure the confidentiality, integrity and security of any personal data held or shared by The University, whatever the medium.

3. This policy applies to 'personal data'. Personal Data is **any** information (including opinions and intentions) which relates directly or indirectly to an identified or identifiable living person. Some types of data are particularly sensitive. Sensitive data includes information such as genetic, biometric or medical/health data, information concerning race, sexual orientation religious or political beliefs and trade union membership. This type of data is special category data and must be treated particularly carefully.

4. The University is subject to restrictions on how it processes personal data and in the handling of personal data is a Data Controller. As a Data Controller, The University responsible for ensuring compliance with the Data Protection requirements outlined in this Policy.

5. The University is fully committed to ensuring continued and effective implementation of this Policy, and expect all Ravensbourne employees, students, associates, third parties and processors to share in this commitment. Any breach of this Policy will be taken seriously and may result in disciplinary action or business sanction.

2. Scope

1. This policy applies to any individual or organisation that processes Personal Data for or on behalf of Ravensbourne or a business affiliated with University activities. Processing of Personal Data includes but is not limited to the identification, collection, recording,

organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure by any means, restriction, erasure or destruction of personal data.

2. This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

3. This policy is designed to establish a worldwide baseline standard for the Processing and protection of Personal Data by all Ravensbourne entities. Where national law imposes a requirement which is stricter than that imposed by this Policy, the requirements in national law shall prevail. Where national law imposes a requirement that is not addressed in this Policy, the relevant national law must be adhered to. If there are conflicting requirements in this policy and national law, please consult with the Data Protection Officer at Ravensbourne (dpo@rave.ac.uk)

3. Purpose and Principles of Data Collection and Processing

1. Ravensbourne needs to collect and store a wide range of Personal Data and Special Category Data about its employees, students and other users of University facilities to allow it to maintain its core operations.

2. Personal data includes staff and student records, alumni data, applicant data, examination marks, research data, electronic data relating to personal devices, images and audio records, residence and catering information, and details of financial transactions. Other information about staff, students and affiliates enables the University to monitor its performance and achievements, and compliance with health and safety and other legislation.

3. To comply with the Act, Ravensbourne must:
    a. Be accountable and transparent in how and why it uses Personal Data;
    b. Demonstrate compliance with the data protection principles;
    c. Allow a person to exercise their Information Rights; and
    d. Adhere to approved codes of conduct for data protection.

4. Data Protection Principles

1. Ravensbourne has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:
    a. **Lawfulness, Fairness and Transparency** - Personal Data shall be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
    b. **Purpose Limitation** - Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes.
    c. **Data Minimisation** - Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed.
    d. **Accuracy** - Personal Data shall be accurate and, where necessary kept up to date.
    e. **Storage Limitation** - Personal Data shall be kept in a form, which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed.
    f. **Integrity & Confidentiality** - Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.
    g. **Accountability principle** – The University must demonstrate that the six Data Protection Principles are met for all Personal Data for which it is responsible.

2. Every person associated with Ravensbourne who Processes or uses any Personal Data must abide by these Principles at all times. In order to ensure that this happens, the University has developed and implemented this Data Protection Policy.

5. Responsibilities

1. As a Data Controller the University is responsible for ensuring that Personal and Special Category Data are collected, stored and Processed fairly, for deciding which types of information will be Processed and the reason for the Processing. The legal responsibility of Data Controller rests with the Vice Chancellor/Chief Executive who is ultimately responsible for implementation.

2. The Executive has allocated the responsibility for the protection of Personal Data at senior management level to a Data Protection Officer (DPO), the University Secretary and Chief Compliance Officer, who is authorised to act independently and has overall responsibility for ensuring ongoing compliance with the University's data protection obligations. The role of the DPO is autonomous and the person that fulfils this role within Ravensbourne reports to the highest level of management within the organisation. The DPO is also the first point of contact for Supervisory Authorities and for individuals whose data is Processed.

6. Senior Management Responsibilities

1. Each Senior Manager is responsible for:
    a. Ensuring that the Personal Data held by that school or service is kept securely and used properly, within the principles of the GDPR;
    b. Advising the DPO of the types of Personal Data held in their school or service, and of any changes or new holdings;
    c. Notifying the DPO of any instances that could be considered a breach of the Act and;
    d. Ensuring that any advice, guidance or instruction issued by the DPO in terms of data protection compliance are given due consideration.

2. Where Processing of Personal Data will involve new technology or high-risk activities, such as sensitive research, a Data Privacy Impact Assessment may need to be conducted. The DPO will act as the authority in this work and will advise relevant staff of when and how such work is to be completed.

7. Staff Responsibilities

1. All staff are responsible for:
    a. Checking that the information that they provide in connection with their employment is accurate and up-to-date.
    b. Informing HR Services of any changes to information that they have provided i.e. changes of address, or of any errors.
    c. Checking that any statements made by the University from time to time about the kind of data kept on staff and students are accurate and up-to-date.
    d. Ensuring that if they Process Personal Data as part of their role they attend data protection training when directed.
    e. Reporting known or suspected breaches of data protection to their immediate line manager.

f. Ensuring that any Processing of Personal Data takes place within the limits of the University's Fair Processing Notices.

8. Student Responsibilities

1. Students must ensure that all Personal Data provided to Ravensbourne is accurate and up to date. They must ensure that changes of address, phone number, next of kin, or any other changes of personal details are notified to Registry by updating their student record online and stating which type of address or detail is being updated (permanent, term-time or next of kin).

2. Students who use the University's computing facilities may process Personal Data as part of their studies. If the Processing of Personal Data takes place, students must take responsibility for that Processing activity to ensure that it is in line with the data protection principles above, and in particular:
    a. The research subject is informed of the nature of the research and is given a copy of the relevant Fair Processing Notice and this Data Protection Policy.
    b. Where consent of a Data Subject is required for Processing that the consent is to be freely given, specific, informed, and unambiguous indication of the Data Subject's wishes.
    c. The Data Subject understands that consent can be withdrawn at any time.
    d. The Deputy Vice-Chancellor is informed of the proposed research before it begins and ensures that the University are authorised to undertake this kind of research.
    e. All information is kept securely using appropriate technical controls – Contact IT Services for guidance

9. Data Security Responsibilities

All staff and students are responsible for ensuring that:

- Any personal data which they hold in whatever format is kept securely;
- Personal information is not disclosed either orally, in writing, electronically either accidentally or otherwise to any unauthorised third party;
- Personal data that is taken off site is not left unattended or unsecured.
- Desks are kept clear of personal data when unattended

Where personal data exists in a manual form, it should be kept in a locked filing cabinet or locked drawer. Where personal data is held in an electronic form, each Dean of School, Director of Service is responsible for ensuring that appropriate technical and organisational measures are taken within the school, service or unit to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, such data.

Examples of such measures include encryption, both at rest and in transit, anonymization and pseudonymising. Each Dean of School or Director of Service is responsible for promoting data protection of best practice within their teams and keeping the DPO informed of changes in the collection, use, and security measures used for personal data within the school, service or unit.

10. Information Rights

1. All staff, students and other users about whom the University processes personal data have rights associated with its use. These rights are:
    a. The right to be informed;
    b. The right of access;
    c. The right to rectification;
    d. The right to erasure;
    e. The right to restrict processing;
    f. The right to data portability;
    g. The right to object; and
    h. Rights in relation to automated decision making and profiling.

2. Where an individual makes a request relating to any of the rights listed above, The University nominated person will consider each such request 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. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative.

3. Data Subjects shall have the right to require the University to correct or supplement erroneous, misleading, outdated, or incomplete personal data. If the University cannot respond fully to the request within 30 days, the DPO or their nominee shall provide the following information to the Data Subject or their authorised legal representative within the specified time:
    a. An acknowledgement of receipt of the request.
    b. Any information located to date.
    c. 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.
    d. An estimated date by which any remaining responses will be provided.
    e. An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
    f. The name and contact information of the appropriate individual who the Data Subject should contact for follow up.

11. Fair Processing Notices

1. Where Ravensbourne act as a data controller, Ravensbourne will provide information to Data Subjects about how their Personal Data will be processed and the purposes for processing. The University will also identify the circumstances under which transfers take place and provide information about routine disclosures to other data controllers. Ravensbourne Fair Processing Notices provide this information for all Data Subjects associated with the University. A complete list of all of Ravensbourne Fair Processing Notices is publicly available on https://www.ravensbourne.ac.uk/about-us/statutory-legal-and-policies/privacy-and-cookies

12. Law Enforcement Requests & Disclosures

1. In certain circumstances, personal data will be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:
    a. The prevention or detection of crime.
    b. The apprehension or prosecution of offenders.
    c. The assessment or collection of a tax or duty.
    d. By the order of a court or by any rule of law.

2. If the University or a known third party processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this Policy but only to the extent that not doing so would be likely to prejudice an investigation.

13. Publication of Ravensbourne Information

1. Information that is already in the public domain is exempt from the Data Protection legislation.
2. Ravensbourne will make public, as much information as is appropriate, about the University's activities. The categories of Information available are set out on in Ravensbourne's Publication Scheme on its Freedom of Information page on the website.
3. Any individual having good reason for wishing details in these categories to remain confidential should advise the DPO who will consult with the Vice Chancellor.

14. Subject Consent to the Processing of Special Category Information

1. In carrying out marketing activities, the University can process personal data only with the consent of the individual. From the date that this policy takes effect, concerns or questions relating to consent should be addressed to the DPO in the first instance.

2. Some posts or programs of study will bring applicants into contact with children, including young people of any age but in any case under 18. The University has a duty under the Children Acts and other legislation to ensure that staff are suitable for the post, and students for the programs offered. The University also has a duty of care to all staff and students and must therefore make sure that employees and those who use University facilities do not pose a threat or danger to other individuals.

3. The University may ask for information about a person's health, particular health needs such as learning support needs, allergies, or any conditions such as asthma or diabetes. The University will only use such information in the protection of the health and safety of the individual or to implement adjustments to support learning or work. The University may also ask for information about a person's criminal convictions, race, gender and family details. This is to ensure that Ravensbourne is a safe place for everyone, or may be to operate other policies, such as the sick pay Policy or the equality and diversity Policy.

15. Data Protection Training

1. All employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training, which will include a data protection e-learning course. For areas that process high volumes of personal data or special category data, bespoke data protection training can be offered. To request more training for Data Protection please contact hr@rave.ac.uk. All staff and students have access to a dedicated data protection intranet site that outlines key responsibilities.

16. Data Sharing and Transfers

1. The University may share or transfer personal data or special category data to internal recipients or other organisations known as Data Processors. In some cases, such transfers may take place to other countries outside of the EU.

2. The University will only share personal or special data where one of the scenarios listed below applies:
    a. The Data Subject has given consent to the proposed transfer or sharing.
    b. The transfer or sharing of data is necessary for the performance of a contract with the Data Subject.
    c. The transfer or sharing is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
    d. The transfer or sharing is required to fulfil a statutory legal obligation.
    e. The transfer or sharing is necessary for the conclusion or performance of a contract to be concluded with a third party in the interest of the Data Subject.
    f. The transfer or sharing is legally required on important public interest grounds.
    g. The transfer or sharing is necessary for the establishment, exercise or defence of legal claims.
    h. The transfer or sharing is necessary in order to protect the vital interests of the Data Subject.

1. Ravensbourne and its entities will only transfer or share personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient and/or data processor. Where third party processing takes place, the department arranging the transfer will first identify if the third party is considered a Data Controller or a Data Processor of the personal data to be transferred. Where the third party is deemed to be a Data Controller, the University will enter into, in cooperation with the DPO, an appropriate agreement with the third party to clarify each party's responsibilities in respect to the personal data transferred.

2. Where the third party is deemed to be a Data Processor, the University will enter into, in cooperation with the DPO, an adequate processing agreement with the Data Processor. The agreement will require the Data Processor to protect the personal data from further disclosure and to only process personal data in compliance with University instructions. All processing of personal data by a Data Processor acting on behalf of Ravensbourne must be documented and new processing activities that involve personal data or special category data should be notified to the DPO who will ensure that the relevant contractual clauses are made available before processing commences.

17. Complaints Handling

1. Data Subjects with a complaint about the processing of their personal data should put forward the matter in writing to dpo@rave.ac.uk. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The DPO or a nominated representative will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

2. If the issue cannot be resolved through consultation between the Data Subject and DPO, or appointed representative, then the Data Subject may, at their own cost, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction. Further information on the complaints process can be provided by dpo@rave.ac.uk.

18. Breach Reporting

1. Any individual who suspects that a personal Data Breach has occurred due to the theft, loss, or exposure of personal data must immediately notify the DPO (dpo@rave.ac.uk) providing a description of what occurred. Notification of the incident can be made via any appropriate means. More information on reporting a Data Breach can be found in the Data Breach Policy.

2. The DPO or an appointed representative will investigate all reported incidents to confirm if a personal data beach has occurred. If confirmed, the DPO will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, the DPO will initiate and chair an emergency response team to coordinate and manage the personal data breach response including notifying the relevant Supervisory Authority if appropriate.

19. Retention of Data

1. The University will keep some forms of information for longer than others, in accordance with legal, financial, archival, or other business requirements. In accordance with the storage limitation principle, the University will dispose of any personal data for which the University no longer has a specified purpose.

20. Research Purposes Exemption

1. Data collected fairly and lawfully for the purpose of one piece of research can be used for other research, providing that the final results of the research do not identify the individual. Such data must not be processed to support measures of decisions with direct consequences for the individual concerned, or in a way that is likely to cause substantial damage or distress to any Data Subject. Records or questionnaires may be kept in order that the data can be revisited and reanalysed. This exemption is only applicable to academic research and cannot be used to provide information about an individual.

21. CCTV & Monitoring

1. Ravensbourne operates a number of CCTV installations that comprise of fixed cameras, printers, monitors, signs, recording and playing equipment, information, material, data, and any ancillary equipment required for the operation of the installations (e.g. cabling, printers, power supplies).

2. The purposes of the CCTV installations are:
    a. The protection of staff, students, visitors, and the assets of the University
    b. The prevention, investigation and detection of crime and disciplinary offences in accordance with the University disciplinary procedures;
    c. The apprehension and prosecution of offenders (including the use of images/data as evidence in criminal / civil proceedings);
    d. The monitoring of the security of premises.

3. The University's CCTV installations will be registered under Ravensbourne's Data Controller registration with the ICO and all release of information will be in accordance with the registration.

4. An exemption to the provisions of the Data Protection Act 2018 covers the disclosure of CCTV for the purposes of:
    a. Preventing or detecting crime; or
    b. Apprehending or prosecuting offenders.

5. This exemption applies only where non-disclosure would be likely to prejudice one of these purposes.

6. In addition to the use of CCTV, Ravensbourne also utilises other monitoring technologies including the use of web monitoring and/or filtering. For further information, please see the University's Security policy.

Appendix A: Document Control

Version	Author	Details	Date	Approved By	Position	Date
1.0	Craig Clark	Initial version	01/06/2018	Data Governance Board	External Consultant	01/06/2018
1.1	Chiz Nwaosu	Minor Updates and Amendments	09/07/2021	Data Governance Board	Privacy Officer	09/07/2021

Appendix B: Supporting Policies

Policy Name
Information Security Policy
Fair Processing Notice Students
Fair Processing Notice Staff

Ravensbourne University London

Glossary

Data Breach – A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Data Controller – The individual or organisation who determines the purposes for which and the means by which personal data is processed. Ravensbourne is the Data Controller.

Data Processor – An external individual or external organisation responsible for processing personal data on behalf of a Data Controller

Data Protection Laws - (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regard to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 2018 ("DPA") and the GDPR (EU 2016/679) and all legislation enacted in the UK in respect of the protection of personal data; and (b) any code of practice or guidance published by the Information Commissioner's Office (ICO) (or equivalent regulatory body) from time to time;

Data Subject – An living individual who can be identified by Personal Data

Personal Data – Any information (including opinions and intentions) which relates directly or indirectly to an identified or identifiable living person

Processing – any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special Category Data – This is Personal Data that needs more protection because it is sensitive. This includes:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Vital Interest – This only covers interests essential to the Data Subject's life