DATA PROTECTION POLICY v7.0

Table of content

1. Revision history

Version	Date	Author	Summary of changes
7.0	March 2025	Diana Stirbu	• Added 'Table of Contents' for easier navigation. • All references to the Data Protection Officer have been changed to Information Governance Manager when appropriate. • Added a clause describing the management framework and roles of the information governance. • Added a requirement for all staff to report requests for access to information within one business day. • The obsolete reference to the Schrems II case was removed. • Added a section describing the requirement to centrally register and "periodically update" the consent of the data subject. • New Artificial Intelligence section added. • Removed obsolete references to the IT security and social media policies. • The audit clause was expanded to further clarify how audits are will monitor compliance. • Some sentences were removed or changed for brevity or greater clarity. clarity for the reader.

2. Introduction

2.1. This policy regulates the acquisition, storage, proper processing, sharing, and disposal of data personal information by Dō University. Hereinafter, in this document, references to the Dō University Group are will simplify to "Group". The scope of this policy includes all persons, information, technologies, resources and facilities that manage information relating to an identifiable person, directly or indirectly indirectly.

2.2. This policy will not form part of the formal employment contract, but is condition of employment that staff comply with the standards and policies established by the Group. Failure to comply with this policy may give rise to disciplinary proceedings.

2.3. Any staff member who believes that the policy regarding the data that is kept about him must raise the matter with the Information Governance Manager. If If you have any questions, you can also consult the Office's website of the Information Commissioner for further information.

2.4. The Group must collect data on its staff, students, clients and other users to be able to monitor their performance, achievements, health and safety. It is also necessary to process this data for be able to pay staff, organize courses and meet the legal obligations to funding agencies and the government.

2.5. Data is also made public through social networks and emails. Therefore, data security transferred by these means is also subject to the principles data protection.

2.6. In the daily management of data, the Group will adhere to the principles data protection prescribed by current legislation in data protection matters and associated regulations.

2.7. It is a requirement that the Group be responsible and can demonstrate the compliance with the detailed data protection principles in section 3.1 below, as well as with the principles, rights and requirements for the processing of personal data from section 3 below.

3. Principles, rights and requirements for the processing of personal data

3.1. The term “processing” in this context has the same definition as Article 4(2) of the UK GDPR.

3.2. The Group must have a valid legal basis for processing personal data. These are:

- Compliance with contractual obligations.
- Compliance with legal or common law obligations.
- To protect someone's life.
- For an organization to fulfill its public task.
- The so-called "legitimate interests", in which the data personal data are used in ways that individuals would reasonably expect to be used and have minimal impact on privacy.

- Explicit consent based on a very clear and specific declaration of consent from the individual. There are other rules surrounding consent, such as requiring explicit consent and simplifying its revocation. Consent should only be used when the Group cannot rely on an alternative legal basis. Consent can be easily revoked with minimal notice.

3.3. All personal data must be:

- Obtained and processed in a lawful, fair and transparent manner.
- They will be obtained for specific and legitimate purposes and will not will be further processed in any way incompatible with these purposes.
- Adequate, relevant and limited to what is necessary in relation for the purposes for which they are processed
- Accurate and up-to-date.
- Stored in a form that allows the identification of the data subjects for no longer than necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures security adequate management of personal data, including protection against unauthorized or unlawful processing, as well as against its loss, destruction or accidental damage, by appropriate technical or organizational measures.
- They will not be transferred to another party, such as a company that processes our data on our behalf or a business partner, unless they can provide evidence that they comply with the principles in section 3.1 and the principles by completing the contract, rights and requirements checklist in section

2. All contracts with such parties shall include standard terms that include compliance with data protection legislation or reference an established data sharing agreement.

3.4. Rights of persons whose personal data are processed by the Group. People have the right to:

- Be informed about the collection and use of your personal data.
- Access your personal data and additional information.
- To have inaccurate personal data rectified or completed if incomplete.
- To have your personal data deleted.
- Request the restriction or deletion of your personal data.
- To obtain and reuse your personal data for your own purposes in different services.
- Object to processing based on “legitimate interests”; to direct marketing purposes and for certain types of investigation.
- To challenge automated decision-making and profiling.

3.5. Personal data breaches

- Everyone involved in the Group has a responsibility to protect the personal data of those who interact with the Group.
- All users of the Group are expected to be attentive to potential violations of this policy. If you become aware of or If you suspect any violation, you must report it. IMMEDIATELY to the person responsible for Information Governance.

• All Group users should be particularly alert to any event that puts their personal data at risk by violating any of the principles in sections 2 and 3.1 of this policy. These breaches are most likely to occur following a security breach of computer systems. However, this is not the only way personal data can be at risk. There are strict time limits for reporting any such breach to affected individuals and the relevant authorities. It is therefore imperative that any actual or suspected breach be reported IMMEDIATELY.

to the person responsible for Information Governance.

4. Notification of data stored and processed

4.1. All staff, students, clients and any person whose personal data the Group processes must:

• Learn what information the Group retains and processes about them and why.

• Know how to access stored data.

• Observe established procedures for keeping data up to date.

• Learn what the Group is doing to comply with their obligations under the Protection of Data and associated regulations.

• Learn how to contact the Information Governance Manager and how to file any complaints with the Information Commissioner's Office.

4.2. Human Resources will request all staff to review annually your personal data stored in the database Human Resources data, using the self-service feature HR

4.3. Students who wish to consult and update their records They should do so by consulting their pastoral tutor or visiting the student center.

5. Staff Responsibilities

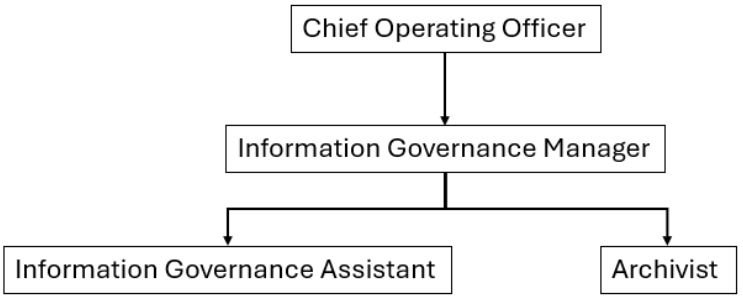
5.1. All personnel shall be responsible for:

- Fully comply with the data protection principles, rights and requirements (3 and 4.1) in data processing personal.
- Conduct a Data Protection Impact Assessment when new data processing is planned personal.
- Immediately raise concerns about data protection or security with the Information Governance Manager.
- Ensure that all data provided to the Group in in relation to your employment are accurate and up-to-date and that changes are made directly in HR Self-Service, where appropriate, or notified to Human Resources using the appropriate forms.
- Review the information that the Group maintains annually and correct any errors.
- All staff are personally responsible for maintain the security of personal data.

5.2. Any personal data of other people that a member of the personal, such as grades or course notes, references to employers or other academic institutions, or any information about personal circumstances must be collected and stored according to the guidelines included in the Manual Personal, the Data Protection Policy and the Policy Record Keeping.

6. Information governance framework

6.1. Group Information Governance is achieved through a structured approach, as described in the following framework:



- The Information Governance Officer is responsible for the Group data protection. For the purposes of Articles 37 to 39 of the GDPR of the United Kingdom, the person responsible for Information Governance is the Group Data Protection Officer.

- The Information Governance Team is comprised of the Information Governance Manager, the Information Governance Assistant, and the Group Archivist. You can contact the Information Governance team throughfrom admin@vae-universityuk.uk or Visiting the Information Governance Office on the Dō University campus.

- Information Asset Owners are relevant staff members responsible for one or more identified information assets.
  Information Asset Owners are described in the Records Retention Policy.

- The Director of Operations is the member of the Leadership Team of the Group responsible for executive oversight of risks information and information risk management.

- The Information Governance Manager prepares monthly reports both to the Director of Operations directly and to the Committee of Systems Integration and Strategy regarding the risks of the information.
- The Chief Operating Officer subsequently reports any significant information risks to the Audit and Risk Committee; the risk level is established in the Information Assets segment of the Group's Operations Risk Register.

7. Data security

7.1. Staff are personally responsible for ensuring that any personal data that you have acquired, managed, processed, shared, stored or deleted:

- All personal data held is stored securely.
- Personal information will not be disclosed, either orally or by written, accidentally or otherwise, to any third party authorized.

7.2. All personal data must be kept in a filing cabinet or drawer. locked. If stored on a computer, they must be stored securely and only to those who have access to them Recommended. Storing personal data on removable media or mobile devices is discouraged, and encryption is mandatory in these cases.

7.3. The official cloud storage solution for personal data is the Microsoft 365 and Docuware Group tenant. It is mandatory to perform a data protection impact assessment before using any other cloud storage service.

7.4. The creation of new computer systems that include the storage of personal information must integrate the privacy in the design process. The design should include, among others other things, the ability to record and manage access of users users to the database and respond to access requests and deletion of data subjects' data.

7.5. Students must ensure that all data provided to the Group are accurate and up to date. Any Changes in data must be notified to the Records Department Students or your Student Department.

Tutor.

8. International data transfers

8.1. The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organizations. These restrictions apply to all transfers, regardless of the size of the transfer or the frequency with which the data is transferred.

8.2. Restricted transfers will only be made when there is a adequacy agreement or the transfer is covered by a adequate safeguards or, in exceptional circumstances, is covered by one of the exemptions of Article 49 of the UK GDPR United Kingdom. No exemption may be applied without consultation previously with the person responsible for Information Governance.

8.3. It should be noted that, following the Brexit transition period, the government of The United Kingdom determines which countries and territories receive the status of adequacy, and these may differ from the adequacy status granted by the European Commission under the EU GDPR.

9. Access to data

9.1. Individuals whose data the Group retains have the right to access any personal data processed about them. The request, known as a Subject Access Request (SAR), must be submitted to the Information Governance team and attach a document of identity (see Annex A). In most cases, the SAR is free. If a charge applies, individuals will be contacted to manage the payment. The SAR must include sufficient information for the Group can find the requested personal data without further effort.

9.2. The Group will endeavor to address all requests for information as quickly as possible.
as soon as possible, but will ensure that, in all cases, the information is provided within one calendar month, unless
the request is considered complex, in which case it will be provided in a within three calendar months.

9.3. Any member of staff who receives or becomes aware of a
SAR, either verbally or in writing, must inform the team
Information Governance. immediately or at least
within one business day of receipt.

9.4. Personal information will never be disclosed over the phone to
external entities or internal personnel other than the
corresponding managers.

9.5. Occasionally, it may be necessary to share personal data with other parties if there is a compelling need and legal justification for doing so, including the protection of the individual's vital interests or if there is a public interest. The method of transfer must ensure the ongoing security of the data and be included in an agreement.

pre-existing (e.g. protective equipment). **Publication**

10. of information

10.1. The Group's policy is to make public as much information as possible.
possible information. The following information will be
available for public consultation:

- Names and photographs of the members of the Corporation.
- Detailed summary of student achievements and exam successes.

Details relating to an individual student are not
will be published without the express permission of that individual.

- Student participation in productions and events related to their studies. Student authorization is required before carry out this activity.

10.2. The Group's internal telephone list will not be a public document.

10.3. Anyone who has good reason to wish that any of these details remain confidential must contact the Governance team of the Information.

11. Subject's consent

11.1. In accordance with Data Protection legislation, the Group will obtain the consent of prospective and new students staff members for data collection and processing, unless there is an alternative legal basis for the processing the same. For sensitive data described in the legislation, will obtain express consent.
This will include information about criminal history and needs. health. In cases where applicants are in contact with children and young people between 16 and 18 years old (or adults at risk), will be carried out verifications, in accordance with current regulations, to ensure who are suitable to work in the Group.

11.2. Consequently, the registration and appointment of staff will be conditioned on the granting of said consent.

11.3. The conditions for consent are set out in the Article 7 of the GDPR. In the event that the consent of the interested party is used as lawful processing of their data personal, the staff must comply with the following:

- adopt clear and direct language when requesting the consent of the interested party.
- The consent of the interested party must be specific and informed, and the interested party must be informed of:

- the name of your organization and the names of any other controller that will depend on the consent (consent to categories of external drivers will not be the sufficiently specific);
- why you want the data (the purposes of the processing);
- what you will do with the data (the processing activities);
- and that people can withdraw their consent at any time, as well as informing them how may withdraw their consent.

11.4. Article 7(3) of the GDPR grants data subjects the right to revoke your consent at any time; in addition, you must be as easy to revoke as to grant.

11.5. The Information Governance team shall also record

consent, which will be updated periodically.

12. Processing of sensitive information

12.1. For the purposes of implementing sick leave, equal opportunities, and other policies, it is necessary to process sensitive information about an individual's health, criminal record, protected characteristics (age, ethnic origin, gender, religion or belief, or disability), and other family data. The Group recognizes that this could cause particular concern or distress and clarifies the reason for the request and the use to which it will be put.

An Article 9 condition, such as explicit consent, is required,

before the collection and processing of sensitive personal data.

13. Data processor

13.1. A "Data Processor" is a person, public authority,

agency or other body that carries out the treatment (which may

consist simply of consulting or maintaining data

personal data on behalf of the Group. For example, a subcontractor

that provides training to our students.

13.2. There must be a contract that stipulates levels of data protection

personal equivalent to those implemented by the Group and

stipulated by data protection legislation. The controller

Information Governance may request a model/annex

contractual for Data Processors.

13.3. Conducting a Data Impact Assessment is mandatory

when there is a risk to the rights of people, before

engage any data controller (see the

Section 17). This includes completing the contract checklist

14. Data Controller

14.1. A Data Controller is an organization that determines the purposes and means of processing personal data (decides why the personal information will be collected and how it will be treated). The The Group is ultimately legally responsible for the application of data protection legislation.

15. Data retention

15.1. The Group will retain some data for longer than others. However, Information about staff, students and other stakeholders cannot be retained indefinitely.

15.2. The Group will maintain an independent retention policy that detail the key categories of data and their duration.

15.3. All data that reaches the end of its retention period conservation will be securely and permanently deleted. This includes both computer files and physical documents.

15.4. Any electronic medium containing personal data must be disposed of safely at the end of its useful life (see (consultations with the IT Service).

15.5. Student records will be retained for a period in accordance with the retention policy. These records include: sensitive information that we are required to collect by government funding agencies. This information includes ethnic origin and may include details about the situation

staff. You can obtain more information from the Governance team of Information.

15.6. Personnel records will be retained for a period in accordance with the retention policy.

Information about pensions, taxes, potential litigation or current employment-related data and the data necessary for the References will be retained for longer periods, depending on the specific circumstances. Documents related to health and security will be retained for longer periods in certain circumstances, such as in the event of problems long-term health.

sixteen. Cookies and similar technologies

16.1. Cookies are small pieces of data that a website download to a computer and allow the website to do so recognize on subsequent visits. They are often used to track visitor activity or for short-term uses, such as shopping cart maintenance.

16.2. Legislation requires that consent be sought for the use of Cookies for certain purposes. The legislation covers not only cookies, but also any technology that can leave data on a person's computer.

16.3. The use of cookies or similar technologies on external Group websites must be assessed in accordance with applicable law to determine whether visitor consent is required.

17. Closed-circuit television (CCTV)

17.1. The Group operates a CCTV system for the safety of staff and the students. The operation of this system complies with the Code of Practice issued by the Information Commissioner. See the CCTV policy.

17.2. Requests for access to CCTV data will be processed in the same way as access to any other type of data personal (see section 7).

18. Transfer of personal data to official bodies

18.1. Occasionally, official bodies such as the Police or the Agency Tax authorities may request disclosure of personal information. Except In cases of emergency, this request will be forwarded to the person responsible for Information Governance or the person designated by it, and

will be assessed in accordance with the relevant provisions of the legislation on data protection.

18.2. All requests for personal data by UK law enforcement agencies must be

Accompanied by a signed application form to a external organization for the disclosure of personal data to the Police Form, also known as DP2. This form is provided by the law enforcement agency. Requests from international law enforcement agencies application of the law must be accompanied by documentation equivalent.

19. Data protection impact assessments

19.1. A Data Protection Impact Assessment is essentially

a risk management process and should be performed before new uses of personal data to identify any problems related to data protection or related legislation.

19.2. Data Protection Impact Assessments must be

formally documented and signed by a relevant person designated by the Data Controller before any new use of personal data.

19.3. In this context, "new uses of personal data" refers to

any use that is not contemplated in the Group's ICO register or in the formal consents obtained from the interested parties.

19.4. The Data Protection Impact Assessment is a stage

mandatory in the prior planning of any new project that involves the use of personal data or in any case in which the

data will be processed by a data processor or a

joint controller on behalf of the Group.

19.5. If you have any doubts about the need for an Assessment of Impact of Data Protection, consult the team Information Governance.

20. Artificial intelligence

20.1. The use of any artificial intelligence (AI) involving personal data must be subject to a full Data Protection Impact Assessment prior to implementation.

20.2. Whenever AI uses personal data, due account must also be taken of Article

22 of the GDPR, which grants data subjects the rightNo to be the object

of decisions based solely on automated processing,

including profiling, if such decisions "produce

legal effects on him or significantly affect him in a

similar".

21. Use of personal data for commercial purposes

21.1. In accordance with Data Protection legislation, the Group

will obtain consent from individuals for the collection and use

data processing for commercial purposes. For sensitive data

described in the legislation, express consent will be obtained.

21.2. Any request for permission to trade with a person must be made with express consent.

21.3. All new proposals for the processing of personal data

for marketing purposes will be evaluated by the person responsible for

Information Governance.

22. Links to other policies

22.1. The acceptable use policy defines specific requirements in terms of data security.

22.2. The Records Retention Policy defines the schedules

retention and describes the requirements for disposal

secure data assets.

23. More information

23.1. For more information on the Data Protection Act of 2018, UK GDPR and EU GDPR, see the website of the Information Commissioner's Office.

24. Protection of Freedoms Act 2012

24.1. The Protection of Freedoms Act 2012 details the obligations

legal requirements regarding the storage, use and destruction of data

biometrics (e.g. fingerprints and DNA).

The Group does not store or use biometric data. The most modern mobile devices,

such as smartphones and tablets, do use biometric data such as

facial and fingerprint recognition. This data is only

stored on the device and must be erased when transferring it to another device

user.

25. Auditing

25.1. The Group will conduct documented audits to verify the

staff compliance with policies and procedures

data protection, as well as with the relevant legislation.

Audits will focus on specific business areas or processes and

will include spot checks on compliance.

25.2. Audits will be supervised by the Information Governance team and will be recorded.

Cases of non-compliance will be subject to controls.

follow-up after an appropriate interval.

25.3. Data processors and joint controllers

data will be audited using a risk-based approach,

proportional to the type and volume of data they process on behalf of the

Cluster.

26. Status of this policy

26.1. The operation of this policy will be reviewed periodically by the Information Governance Manager.

26.2. This policy may be reviewed and modified periodically by the Team

Group Leadership.

Annex A

Acceptable forms identification

To verify the identity of a person requesting personal information, a form must be provided identification of each category.

Photo ID

- Driving license
- Passport
- Armed forces identity card

Proof of address

- Recent bank statement or utility bill, etc.

Policy Review Area	HE
Senior Manager/Owner	JOSEP FABRA SEGARRA
Approval level	Group/Corporate Leadership Team
Approval date	MARCH 2025
Review cycle	Every five years
Next review	March 2030