UNIVERSITY OF PORTSMOUTH

DATA PROTECTION POLICY

October 2021

Contents

Document title
Data Protection Policy September 2021
Document author and department
Samantha Hill, Information Disclosure and Complaints Manager (and the University's Data Protection Officer), Office of the Executive Director of Corporate Governance
Approving body
Executive Director of Corporate Governance
Date of approval
20 September 2021
Review date
June 2024
Edition no.
9
ID Code
022
Date of effect
1 October 2021
EITHER For public access online (internet)? *Tick as appropriate* **YES ✓**
For public access on request copy to be mailed *Tick as appropriate*
OR For staff access only (intranet)? *Tick as appropriate*
Password protected *Tick as appropriate* **NO ✓**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk If you need this document in an alternative format, please email corporate.communications@port.ac.uk

The latest version of this document is always to be found at:

UNIVERSITY OF PORTSMOUTH

policies.docstore.port.ac.uk/policy-022.pdf

Summary

What is this document about?

This policy document sets out the University's commitment to adhering to the data protection principles of the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the EU GDPR. This policy sets out the responsibilities of everyone who handles personal and special category data within the University.

Who is this for?

This policy will be of interest to anyone whose personal data is processed by the University, including but not limited to, applicants to work or study at the University, current staff and students, former employees and alumni, research participants and visitors to the University.

It is also of importance to all staff within the University who process personal, or special category, data within or on behalf of, the University.

This policy will also be of interest to the wider public in relation to how the University processes personal data generally.

How does the University check this is followed?

Information Governance staff make information about data protection available on the University website and intranet, and by training staff on data protection principles with examples of good practice. The University encourages staff to raise questions about data protection matters and to report any issues or data breaches they may come across in their work. From the take up of training opportunities, the knowledge shown by staff and the questions asked, the University believes the policy is being followed.

Who can you contact if you have any queries about this document?

All enquirers may contact the University's Data Protection Officer, Samantha Hill, on 023 9284 3642 or data-protection@port.ac.uk .

Executive summary

The Data Protection Policy sets out the University's commitment to complying with the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018), the EU GDPR (in cases where the University has customers in the EU) and complementary legislation. This policy notes the actions the University will take to fulfil its legislative obligations and the responsibilities of staff and students in relation to personal data. The policy applies to all individuals who may process personal data held on behalf of the University and will be of interest to all students, staff and other individuals about whom the University might process personal data.

The main points of the policy are:

1) It is necessary to process personal data relating to students, staff and other individuals in order to be able to carry out the proper functions of an educational institution engaged in teaching, research and as an employer.
2) The University and its staff will adhere to the data protection principles as set out in the UK GDPR, the DPA 2018 and complementary legislation.
3) The University will publish information on its website about the personal and special category data that it processes in line with Article 30 of the GDPR and will keep this information up to date. The University's registration number with the Information Commissioner's Office is Z7027819.
4) The University is required to have a Data Protection Officer. This post is held by the Information Disclosure Manager.
5) All staff, students and other individuals have the right to access details of their own personal and special category data processed by the University.
6) Students and staff must provide the personal data required by the University as part of the contract they enter into to either administer their education, or to facilitate their employment, and must keep this data up to date using the student or staff self-service portals. If any details that are not included on the portals need to be updated, students should contact their own academic school / department and staff should contact HR to change these further details.
7) It is the responsibility of managers to ensure their staff are aware of the requirements of the data protection legislation when processing personal data.
8) Training in information governance matters is available to all staff from the induction process onwards. Managers should ensure all staff who are new to the University have successfully completed the induction training within three months of joining the University, and that staff who have just moved to a new post have updated their Information Governance training knowledge within one year of joining their new post.
9) Any personal data breaches must be notified to the University's Data Protection Officer and / or Information Security Architect as soon as possible after discovery, so that a decision on notification to the Information Commissioner's Office is made within the stipulated 72 hours.
10) Any deliberate or negligent breach of the requirements of the data protection legislation may result in disciplinary action being taken against the relevant member of staff or student.

Many of the terms used in this policy are taken from the UK GDPR and DPA 2018. A full explanation of the terms can be found at Annex A to this policy.

This policy should be read in conjunction with the documents and policies listed in Annex B to this policy, all of which can be found on the University webpages and intranet.

Data Protection Policy

1. Introduction

1.1 As a centre for knowledge, research, education and training, much of the University's work involves information and its use. For educational, research and administrative purposes, much of this information will relate to living persons – it is their personal data. The University needs to collect and keep personal data about its employees, students and other individuals to allow it to operate effectively and efficiently: for example, to consider applications from students, enrol students, monitor performance, to assure health and safety and to monitor equal opportunities. It is also necessary to process data so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government properly met. The University is committed to protecting the personal data that it processes in ways that protect the rights and freedoms of the individuals to whom the data relates.

1.2 To comply with the data protection legislation, such processing of personal and special category data must have a legal basis, be collected and used fairly, stored securely and not disclosed to any other person unlawfully. The principles to ensure that personal data is processed properly, and which the University follow to ensure it complies with the legislation, are that the data shall:

1.2.1 Be processed lawfully, fairly and in a transparent manner;

1.2.2 Be obtained for specified, explicit and legitimate purposes and not further processed in a manner that is at odds with those purposes (unless for archival, scientific or historical research purposes or statistical purposes);

1.2.3 Be adequate, relevant and limited to what is necessary;

1.2.4 Be accurate and, where necessary, kept up to date;

1.2.5 Not be kept in an identifiable form for longer than is necessary for the purpose for which it was collected;

1.2.6 Be kept safe from unauthorised access, accidental loss, damage or destruction, and,

1.2.7 Not be transferred to a country outside of the EEA without appropriate safeguards being in place.

1.3 The University and its staff who process personal data will ensure that they follow these principles at all times.

2 Responsibilities and ownership

2.1 The University as a corporate body is the data controller for all processing of personal data carried out under the data protection legislation. The Board of Governors is therefore ultimately responsible for implementation of the data protection legislation, ensuring that the University complies with the legislation. Responsibility for the overall management of the implementation of the legislation lies with the Executive Director of Corporate Governance, who vests day-to-day responsibility for implementing the provisions of this policy with the University's Data Protection Officer.

2.2 The University is a public authority as defined by the Freedom of Information Act 2000 and as such is required, under Article 37 of the GDPR, to have a Data Protection Officer (DPO). This work is carried out by Samantha Hill, the Information Disclosure Manager

2.3 The DPO is responsible for raising data protection issues within the University, providing advice and training to staff (and students), advising on the need for assessments to be carried out under the legislation and monitoring University compliance with the legislation. The DPO is also

responsible for responding to requests for personal data or the application of data subject rights received by the University (or for advising others on how to respond appropriately) and for liaising with the Information Commissioner's Office (ICO). The DPO will prepare an annual report on this work for the Information Governance group and the Board of Governor's Audit and Quality committee.

2.4 As an organisation that processes personal and special category data, the University is required to pay a data protection fee to the ICO. The University provides the ICO with certain information to determine the level of the data protection fee payable and from that, the ICO will publish contact details for the University and for the University's Data Protection Officer, fee information, any trading names used by the University and the data protection registration number given by the ICO (Z7027819).

2.5 The responsibilities of staff and students under this policy are outlined in sections 5 and 6 respectively below. Failure to follow the policy may result in disciplinary proceedings being brought by the University, whilst deliberate breaches of the data protection legislation may result in action being taken against the individual by the ICO, the supervisory authority for this legislation.

2.6 Any individual who considers that the policy has not been followed in respect of their own personal data must raise the matter initially with the University's Data Protection Officer. If the member of staff or student is unhappy with the steps taken by the University to resolve their issue, that individual retains the right to make a complaint to the ICO.

2.7 Any individual who believes that this policy has been contravened to the point that a data breach has occurred, should use the process outlined in the Data Breach Notification policy. See section 9 below for further information.

3 Records of data held and processed by the University

3.1 The University will maintain and use records of personal and special category data relating to staff, students and applicants to the University as is necessary and appropriate for its effective operation as an educational organisation, employer and research institution. Those who are offered study places or posts for employment at the University will be notified of the standard data kept about them on acceptance of these offers. Copies of the general data protection statements that set out why the data is needed, the University's legal basis for processing the data, how the data will be stored and how long it will be retained before destruction are available here. Where, in addition to this central collection of personal data, personal data is collected about particular groups of students or staff for specific purposes, such as for field trips or research purposes, this will be separately notified on a group or individual basis as appropriate, by the department processing that data.

3.2 The University maintains a record of the data processing carried out across the University in accordance with Article 30 of the GDPR. This record contains the following information:

- Name and contact details of the University and of the University's Data Protection Officer
- Purposes of the processing and a description of the people from whom personal data is collected and the types of data collected
- Details of third parties with whom the personal data might be / has to be shared
- Whether data will be transferred outside of the European Economic Area
- The retention periods for the different types of personal data processed by the University
- A general description of the security measures taken to keep data safe

- What special category and criminal offence data is processed by the University, and under which particular specified conditions

An extract from this record can be found on the University's Information Governance webpages.

3.3 The University must have a legal basis for its processing of personal data, as set out in Article 6 of the GDPR. Each of the legal bases in Article 6 may apply to the processing carried out by the University at any time, but those bases that the University will rely on most are:

- That the processing is necessary for the performance of a contract with the individual to whom the data relates
- That the processing is necessary for the compliance with a legal obligation on the University
- That the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the University
- That the processing is necessary for the purposes of the University's legitimate interests (although only in relation to certain of the University's activities)
- That the individual has given their consent to the processing

3.4 It is necessary for the University to process special category data to operate or monitor University policies (e.g. sick pay, equality and diversity, to make the appropriate relevant adjustments for staff or students), to ensure the University is a safe place to work or study, or to enable the institution to comply with the law. To process this special category data, the University is required to have additional legal bases for this processing, as set out in Article 9 of the UK GDPR, separate from those required to process personal data. The further legal bases that the University will rely on most are:

- That the data subject has given explicit consent to the processing
- That the processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or the data subject in the field of employment
- That the processing is necessary for the establishment, exercise or defence of legal claims
- That the processing is necessary for reasons of substantial public interest
- That the processing is necessary for the purposes of preventive or occupational medicine
- That the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats
- That the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- That the processing is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained (DPA 2018 Schedule 1 Part 2 s8).

3.5 It is recognised that in some circumstances the processing of such data may be a matter of particular concern to individuals. Accordingly, where possible the University will anonymise this data as soon as possible: for example, where the data is only required for monitoring purposes. Where it is necessary though to keep this data in a way that identifies the individual to whom it relates, staff and students will be made aware of the sensitive nature of the information they are being asked for and will be asked to give separate explicit consent for the use of this data. The one exception to this would be if a situation occurred where there were concerns for the safety of the individual or another person. In such a situation, the GDPR allows special category data to be

processed without referral to the individual in advance, where that person is incapable of giving their consent.

3.6 Students are formally asked to check the accuracy of their personal data annually at enrolment. Staff are formally asked to check the accuracy of their personal data at least once every two years. Students can update their data at any time through MyPort, whilst staff are able to update their HR records at any time through the employee self-service online system (ESS).

4 Data Protection 'Rights of the Data Subject'

4.1 All individuals whose personal data is processed (a data subject) have rights under the data protection legislation in relation to the processing of their personal data. The University will respond to all requests to exercise any of these data subject rights as soon as possible and within a calendar month of receipt of the request. The following is an explanation of the data subject's rights and their application:

Subject Access Rights

Individuals have the right to know how their personal data may be processed (see information on data protection statements at section 3.1 above) and to access any personal data that is being kept about them by the University. Further information on the Subject Access Request process, what information will be accessible and how to receive copies of their personal data is available here.

Right to rectification

If an individual believes that the University holds inaccurate personal data about them, they have the right to require that data to be rectified, or to have an additional statement added to that data to explain what is wrong.

Right to erasure (to be forgotten)

Individuals have the right to have personal data relating to them erased from the University's systems in the circumstances listed below.

Personal data must be erased on request

- Where it is no longer necessary for the personal data to be held
- Where the consent given for the processing is withdrawn (and no other legal basis exists for retaining the data)
- Where the individual objects to the processing for public and legitimate interest reasons [unless the University can prove compelling legitimate interests to continue the processing]
- Where the personal data was processed unlawfully in the first place
- Where the personal data must be erased in compliance with a legal obligation, and
- Where the personal data was collected in relation to marketing, creating user profiles and collecting personal data from children under the age of 13, via the internet.

However, the legislation also allows for situations where the right of erasure may not be applicable (Article 17(3)): for example, where the processing is necessary for exercising the right of freedom of expression and information, complying with a legal obligation, for reasons

of public interest in the area of public health and for the establishment and exercise of legal claims, so this is not an absolute right.

Right to restrict processing

Individuals can require the University to restrict processing of their personal data; that is, temporarily stop or no longer allow any future processing of their personal data, in situations where:

- The accuracy of the personal data is in question
- The processing is unlawful but the individual does not want the data erased
- The University no longer needs the personal data but the individual requires its retention for legal reasons, or
- The individual has objected to processing based on the legal basis of public or legitimate interests.

Once an individual has exercised this right, the data can only be processed subsequently with the individual's consent.

Right to data portability

Where an individual has given their *consent* to the processing of personal data that they have provided in an electronic form to the University, and the processing is carried out automatically, the individual has the right to either receive a copy of that same data in a machine-readable format or to have that data transmitted directly to another data controller.

Right to object

An individual can object to the processing of their personal data in the following circumstances:

- When the processing is based on the legal basis of either being in the public interest or the legitimate interests of the University
- Where the processing is for direct marketing purposes
- Where the processing is for scientific or historical research purposes, or statistical purposes – unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Right not to be subject to automated decision-making

Individuals have the right not to have decisions made about them solely through automated processing where that decision will have a legal effect. The University will implement suitable measures to safeguard the rights and freedoms of the individuals, such as engaging human intervention in the process.

4.2 For more information on, and to exercise, any of these rights, please contact the University's Data Protection Officer, using the contact details in the Summary section of this document.

5 Responsibilities of staff

5.1 All staff have the following responsibilities:

- To check, when requested, that any data they provide to the University in connection with their employment is accurate and up to date. This can be done through the University's HR self –

service function, ESS.

- To inform the University of any changes to, or errors in, the data held
- To comply with the guidelines for staff in section 5.2 below if and when, as part of their responsibilities, they process data about other people.

5.2 Staff whose work involves the use of personal data are responsible for ensuring that:

- They have read and follow this policy, the Data Breach Notification policy and the other policies listed in Annex B to this policy
- They have undertaken the Information Governance eLearning training and updated their knowledge, at least every two years
- When collecting personal or special category data, they collect only the minimum amount of data necessary to complete the work for which the processing is necessary (the concept of data minimisation)
- They provide sufficient information to explain the reasons for the data processing (see section 3.1 above)
- They carry out a Data Protection Impact Assessment (DPIA) whenever necessary (see section 9 below for more information on DPIAs)
- They anonymise personal data as soon as possible and wherever appropriate
- When employing a third party as a processor, that third party is made aware of their responsibilities under the UK GDPR (see section 10) and ensure that these are captured in appropriate contractual documents
- Any personal data that is held in hard copy or electronically is kept securely either in locked cabinets or through the use of password protection and encryption of electronic files where necessary. Further appropriate controls include access controls and anonymisation
- Personal data is not disclosed by them orally or in writing, to any unauthorised third party, including family members
- The personal data for which they are responsible is accurate and kept up to date where appropriate, held for the appropriate length of time and destroyed confidentially when / if it is no longer needed, in line with the University retention schedule
- They do not access any personal data which is not necessary for their work; and
- If working remotely from the University, they maintain the same levels of physical security for personal data and the equipment that the data may be stored on or accessed through as if they were working on campus. Electronic versions of data must be stored on University systems, not on personal drives or equipment.

5.3 Managers have an additional responsibility to ensure that their staff are aware of the data protection principles (see section 1.2 above), and know how to correctly process personal and special category data as part of their work. Managers should also ensure that their staff have taken the Information Governance eLearning module on the University's Moodle site – this is mandatory for all staff and forms part of the core staff training (see section 15 below for further information).

5.4 Any deliberate or negligent breach of these responsibilities – or of the statutory obligations of the GDPR – may result in disciplinary action being taken against the relevant member of staff.

6 Responsibilities of students

6.1 Students must assist the University in ensuring that all their own personal data provided to the University at registration is accurate and up to date. Students who need to notify the University of any subsequent changes in their personal details can do so via the My Details tab on their MyPort account which can be accessed via the myport.ac.uk address.

6.2 Students may themselves need to process personal data for project or research purposes (for example, in carrying out surveys) or they may be employed by the University in a part-time job that handles staff or student personal data.

6.3 If students are carrying out projects or research work they must notify their personal and project tutors and obtain the agreement of their Faculty Ethics Committee to the need to process the data before starting the collection of any personal data. Part of the submission to the Faculty Ethics Committee must contain details of how long the personal data will be held, in which format, and how it will be destroyed. Any reporting based on personal data collected during research must be done anonymously unless the research participant has agreed in writing to their personal data being used in such a way as to identify them.

6.4 Students employed by the University in positions that allow access to personal data about any student, applicant or member of staff must abide by the responsibilities for staff as set out in paragraph 5.2 above and take care not to access any personal data about anyone not directly related to the work being carried out.

6.5 It is good practice, where a student is employed as a member of staff, for the student's access to personal data to be restricted only to areas of the University in which they do **not** work or study or know any students. If a student becomes aware that they know an individual whose data they are required to access, the student must inform their line manager as soon as possible. The line manager will determine whether there is another way for the student to carry out the work, or may move the student to another area of work, to avoid any complications.

7 Use of personal data in research

7.1 Whilst one of the principles of the data protection legislation is that personal data shall not be processed for any reason other than the purpose for which it was collected (Article 5.1.b.), further processing, without requesting the data subject's consent to the further processing, for research or statistical purposes is allowed under Article 89(1), so long as safeguards for the rights and freedoms of the individual concerned are implemented.

7.2 These safeguards include the idea of data minimisation, pseudonymisation or anonymisation of the data to reduce the possibility of identification of the individual.

7.3 Once personal data has been anonymised to the point where a living individual can no longer be identified by it, the data ceases to be personal data and therefore the constraints of the GDPR no longer apply.

7.4 Personal data used in research cannot be processed in a way that will have a direct effect or result on the identifiable individual, or in such a way as to cause damage or distress to the

individual. These adverse effects are generally avoided by the anonymisation of the data before being used for research, as noted above.

7.5 The legal basis for processing personal data in most research projects will be that the individual has given their consent to the processing. It may be the case, however, in some NHS research projects, that the legal basis for the processing is that it is necessarily in the public interest. For more information on this point, please contact the University's Ethics Advisor.

7.6 It is important when recruiting participants for research projects, to reassure them that their data will be processed in accordance with the UK GDPR and that they have the right to see the data that is held about them, unless it has been anonymised so that they can no longer be identified. This information should be given to participants in a durable format prior to the start of their involvement in the research (for example, the Participant Information Sheet), so that they are aware of the extent of the processing prior to taking part in the research, and so that they may refer to it after their participation in the research activity is complete.

7.7 Further information on managing the use of personal and special category data in research is available from the Research Outputs Team based in the University Library, or from their webpages.

Research and Innovation involving third parties

7.7.1 Personal data should only be provided to third parties if this has previously been agreed by the data subjects. There must be a written agreement in place to govern the deployment, ethical use, integrity and security of the data. This written agreement must also stipulate the third party's obligations to retain the data for a defined period of time, and to destroy the data when it is no longer needed. There must also be procedures in place to ensure that the transfer of all personal data is secure.

7.7.2 If personal data that has been provided by another organisation is to be used in a research project, steps must be taken to ensure that the research is compatible with what the data subjects were told would happen to their data, unless the personal data is anonymised to the point where the individuals cannot be identified by the data.

7.7.3 Activities that involve third parties who are contracted to secure or collect data on behalf of the University must be carried out according to the principles set out in the University Ethics Policy as well as this policy.

8 International transfers of personal data

8.1 Transfers of personal data to countries outside the UK are deemed to be international transfers. Despite the fact that the UK has left the EU, transfers to member countries of the EEA are made legitimate by the adequacy decision adopted by the EU on 28 June 2021. This decision affirms that the UK's level of protection for the personal data of EEA citizens is adequate for the EU's purposes and therefore transfers of personal data between the UK and the EEA can continue as if the UK was still part of the EU. The adequacy decision is time limited, that is, it will automatically expire on 27 June 2025, so it will be necessary to ensure that policies are in place to account for this in contracts, in case any application to extend the time period is not granted.

8.2 Transfers of data outside of the EEA are considered to be transfers to 'third countries' and can only be made when appropriate safeguards of the data and the rights and freedoms of the data subject

have been provided. For the purposes of the University, the most appropriate safeguard (unless there is a legally binding and enforceable instrument between public bodies) is the use of Standard Contractual Clauses relating to the processing of personal data in the contract with the organisation in the third country. The EU adopted new Standard Contractual Clauses in April 2021 which can be used with immediate effect. The ICO is also preparing UK specific contract clauses and staff should preferably use these, when drafted, when preparing contracts involving personal data processing with an organisation in a 'third country'. Further information about these clauses and when they can be implemented will be available from the University's Data Protection Officer.

9 Electronic Marketing

9.1 In addition to ensuring that the data protection principles are adhered to when engaging in electronic marketing, staff also need to be aware of the need for compliance with the Privacy and Electronic Communications Regulations (PECR). The PECR essentially cover the use of *unsolicited* marketing messages sent by electronic means including telephone calls, texts, emails or any other electronic means and the use of cookies, or as it becoming more common, tracking pixels. The PECR apply even when personal data is not involved, for example when emails are sent to companies.

9.2 *Solicited* marketing is that which has been requested. For example, a response to an email requesting information about a course is a solicited / requested marketing response. *Unsolicited* marketing is any message that has not been specifically requested, such as emails advising individuals of new initiatives, but it is still possible to send these messages, so long as the actions comply with PECR.

9.3 The best way of being compliant with PECR is to have the individual's consent to being sent further messages which can be collected either when the first contact is made, or as soon after as possible. That is, if staff are attending a conference and collect the names and contact details of individuals for a particular issue, it would be best practice to ask the individual at this point to indicate their preferences to be contacted in future – whether they want to be contacted and the method of contact e.g. telephone, email – and to give their consent to this further marketing. If there is not enough time to do this, then a single email should be sent as soon as possible after the conference, explaining how the individual's details were collected and asking them to indicate their preferences in, and consent to, receiving further correspondence. In cases where an individual declines to receive any further marketing a note should be kept of this decision so that the individual is not contacted again. Where an individual indicates their agreement to receiving further correspondence (by 'opting in'), further communications can be sent, but each one should include an easy way to unsubscribe from further messages. In this way, the communications are compliant with PECR.

9.4 A second way of being compliant with PECR is that electronic mail marketing can be sent to an existing customer of the University – that is, someone who has previously received a similar service or product from the University. In order to be compliant, the customer must have been given a simple way to opt out when their data was first collected and in all following correspondence, they must be given an easy way to unsubscribe.

10 Data Protection Impact Assessments

10.1 The GDPR requires data controllers to complete an assessment of potential risks to the rights and freedoms of individuals when either new technologies are used for data processing, where

large amounts of special category data are processed or where automated decisions (including profiling) will take place that will lead to decisions that can have a legal effect on the individual. This assessment is a Data Protection Impact Assessment.

10.2 A Data Protection Impact Assessment (DPIA) should be started as early as possible in a project, and revisited at key stages in the project - at review points or milestones - or as and when changes to the project take place. This is necessary to ensure that the data protection principles and the rights of the data subject remain central principles in all applicable projects. The assessment process includes the appropriate consideration of privacy by design, the level of security needed for the personal data being processed, and the proper management of the data when it is no longer needed, either through anonymization or destruction. Any risks identified through the assessment are considered and where possible, actions taken to mitigate the risk. Any remaining high-risk processing must be escalated to senior staff for their knowledge / understanding and authorisation.

10.3 The University has a process and a DPIA template for carrying out the required assessment. Further details are available from the University Security Architect, Robbie Walker on Robbie.walker@port.ac.uk .

11 Data Breaches

11.1 The University has a Data Breach Notification policy which must be followed if anyone believes that there has been a personal data breach: that is, a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A serious data protection breach must be notified to the Information Commissioner's Office within 72 hours of becoming aware of the breach, so staff must know how to deal with a data breach.

11.2 A data breach must be reported to the Data Protection Officer or the Information Security Architect via the Data Breach notification form, after which action to minimise or contain the breach must be taken as soon as possible. More detail on this process is available in the Data Breach Notification policy.

12 Data Processor responsibilities

12.1 The responsibilities associated with being a data processor (that is, a third party that carries out data processing actions on behalf of, and on the instructions of, a data controller) must be pointed out to the data processor at the beginning of a contract between both parties.

12.2 If a data processor is employed to carry out work on behalf of the University, staff involved in the contract must ensure that it sets out the University's own responsibilities in relation to the data processing (the instructions for processing and security requirements of the data processor) and contains the following information in relation to the data processor's responsibilities:

- the fact that the data processor can only process data in the ways set out in the contract
- the fact that the data processor's staff must be trained in secure data processing methods and understand the confidentiality aspects of their work
- that appropriate security measures are taken for the personal data being processed

- that the processor can only engage a sub-processor with the agreement of the University and on the terms required by the University
- that the processor provides assistance to the University in dealing with data subject rights, where requested by the University, and
- that the data processor either deletes or returns the personal data to the University at the end of the contract.

12.3 For further information on including these requirements in contract terms please contact the University's procurement team on finance.purchasing@port.ac.uk.

13 Publication of University data

13.1 As a public authority, the University is required, under the Freedom of Information Act 2000 (FOIA), to make publicly available information about the University and the way it is run. The University does this through its publication scheme and by answering requests made under the FOIA. Staff who receive a FOI request can respond to the request themselves if the response is something they would usually handle themselves, but any complex requests should be forwarded to colleagues within the Information Disclosure team.

13.2 Personal data will not normally be included in a response to a request or in the published classes of data in the Publication Scheme unless names are given to identify a member of staff as a contact for any particular part of the University's business or where the personal data is part of a webpage established by a Department / School or Service.

13.3 If the University receives a request for data about a member of staff, the University is only required to release information relating to the individual in a business capacity. Anything relating to that individual's private life (which for most staff members will include precise salary details) will not be disclosed by the University.

13.4 The University will generally only disclose 'personal business' data in the following situations:

- Where the request relates to senior members of the University – that is, all Directors / Heads of Department, Schools and Services and above, including Governors. Staff of a more junior level will not normally have any data about them disclosed.
- Where the role of the individual in the information requested is significant, e.g. the name of the person acting on an issue may be disclosed but the name of an individual who simply forwarded an email to that person will not be disclosed.
- Where the extent of the public funding involved is significant – the purpose of the FOIA is to make public authorities more transparent and accountable for their decision making. Where individuals are associated with decisions about large sums of the University's funds, their details may be released.

13.5 In the event that a request for information about a member of staff or a Governor is received by the University, the need to disclose any data will be discussed with the member of staff or Governor before any information is disclosed.

14 Retention of data

14.1 The University is committed to keeping and disclosing personal data in a responsible and secure manner and will therefore keep data for the minimum time necessary to fulfil its purpose.

14.2 The University will keep enough data about a **student**, to be able to confirm the qualifications achieved whilst at the University, for 80 years from the date that a student graduates or withdraws from the University. Any other data will be removed from student files six years after the student graduates or otherwise leaves the University. For further details of the retention of student data please see section 11 (Student and Course Records) of the University Retention Schedule.

14.3 The University will keep basic employment history data about former **employees** for 100 years from the staff member's date of birth in order to verify employment details. Most other data will be removed a minimum of six years after their employment with the University has finished, in order to meet data needs for pensions, taxation, potential or current disputes or job references. For further details on the retention of staff details please see section 6 (Human Resource Records) of the University's Retention Schedule.

14.4 The University will also keep the health and safety records of accidents that happen to visitors to the University for three years after the date of an accident.

14.5 Personal data that is no longer required will be destroyed in as secure a manner as possible. Paper based records will, at least, be put in a confidential waste sack or confidential waste bin for collection as soon as possible by the secure waste collection contractor or, preferably, shredded on site. Electronic records will be deleted if hardware such as hard drives, laptops, smart phones, photocopier / printers etc are decommissioned. The Printing Services Team of the Marketing and Communications department of the University is responsible for the deletion of data held on multi-function devices when they are decommissioned and the IS department has a contract with a third-party organisation to dispose of redundant electronic equipment. Further details are available from the University's Information Security Architect.

15 Training

15.1 It is the responsibility of the University to ensure that staff are aware of the data protection principles, standards and responsibilities, and it has therefore produced the Information Governance eLearning training module accessible via the University's eLearning site (Moodle). This training package also covers topics relating to the freedom of information legislation, records management and information security. The training module is core training and therefore must be taken by all members of staff.

15.2 Members of the Information Governance team also present a range of training sessions on Information Governance issues including data protection and records management, a Management Information Briefing session on information governance subjects, and compile a regular IG newsletter updating staff on IG matters. Details of the content of, and dates for, IG training can be found on the Information Governance webpages.

15.3 Staff in the Information Governance team are also happy to provide bespoke training for groups / departments – should you wish to discuss further training requirements please send an email to information-matters@port.ac.uk .

16 Conclusion

16.1 Compliance with the GDPR and the Data Protection Act 2018 is the responsibility of all

members of the University. Any breach of this Data Protection policy may lead to disciplinary action being taken, or access to University facilities being withdrawn, or in the most serious circumstances, a criminal prosecution.

16.2 Any further questions or concerns about the interpretation of operation of this policy should be raised in the first instance with the University's Data Protection Officer.

Annex A – definitions of terms used in this policy

The terms used in this policy are taken from the UK GDPR and the DPA 2018.

Personal data: any information relating to an identified or identifiable living individual, including by reference to an identifier such as an ID number, location data or online identifier. Personal data includes special category data as described below

Special category data: personal data relating to issues of:

- the racial or ethnic origin of the data subject
- political opinions
- religious or philosophical beliefs
- trade union membership
- physical and / or mental health
- sex life or sexual orientation
- genetic or biometric data processed for the purposes of uniquely identifying a living individual
- criminal convictions or offences (by virtue of s10 of the DPA 2018)

Processing: the collective term for any action or set of actions relating to personal or special category data, including collecting, recording, organising, adapting, altering, storing, using, disclosing, erasure and destroying data. Processing also includes the transmitting or transferring of data to a third party

Data Protection legislation: the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the EU GDPR.

Data subject: the individual who is identified by the personal data collected

Data controller: the organisation that determines (alone or jointly with others) the need, purpose and means of processing personal data, and the uses to which it will be put. All departments, schools and sections of the University form part of the legal entity which is the University, which is itself, the data controller

Data processor: a third party which processes personal or special category data on behalf of a controller

Data Protection Impact Assessment: a risk assessment of any new processing, to protect the rights and freedoms of the data subject whilst allowing the data processing to continue

Data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Third party: any external person or organisation that is neither the data subject nor the data controller

Pseudonymisation: the processing of personal and special category data in a way that the data can no longer be attributed to a specific data subject without the use of additional information, which itself must be kept securely and separately from the pseudonymised data.

ICO: the Information Commissioner's Office, the UK supervisory authority for, amongst other things, the data protection legislation.

Annex B – related information

This policy should be read in conjunction with the following documents and policies, all of which can be found on the University webpages and intranet;

- ICT Acceptable Use policy
- Various Information Security advisories
- Data Protection statements for applicants, students and graduates, and staff
- Data Breach Notification policy
- Research Data Management policy
- Freedom of Information webpages
- Records Management webpages
- Email policy (Staff)
- Email policy (Student)

Annex C - Data Classification Schema

What kinds of data must be protected?

Any item of information relating to the business or interests of the University is an information asset. This includes strategy documents, research papers, student applications, staff contact details, course materials, results data etc. If these assets were compromised, then the impact could be potentially damaging to the University (including damaging reputation) and detrimental to students or staff.

Impact potential

Not all information assets have the same 'impact potential' and therefore do not need the same protection. For instance, it would be a nuisance and a waste of resources if we applied the same security controls to routine correspondence as we do to sensitive medical reports. It is important to understand the 'impact potential' and know the location of our information assets. Without this knowledge, we do not know how much time, effort and money to spend on security.

If read by unauthorised persons, lost or damaged then some data has the potential to:

- Harm academic relations
- Breach copyright
- Cause considerable departmental embarrassment
- Cause considerable inconvenience to staff or students
- Damage operational effectiveness or security
- Cause considerable financial loss
- Facilitate fraud, improper gain or advantage for individuals or third parties
- Jeopardise an investigation
- Facilitate the commission of crime
- Undermine the proper management of a department / school / service

By understanding the impact potential and classifying the data on that basis, the University can suggest the most effective ways to handle this information – in terms of backup, encryption, rules for safe transmission and disposal etc. Classifying data enables us to focus resources on its protection more effectively.

There are three types of information which are classified as RESTRICTED.
Personal data

Personal data identifies a living individual. For example, a name accompanied by other data about the individual such as address, age, email address (including work email addresses), telephone number, data regarding his / her financial status.

Personal data can be an expression of opinion about the individual and can include any indication of the intentions of the data controller in respect of the individual.

Special category data

Personal data which identifies a living individual and includes any of the following types of data about that individual is considered to be special category data:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership

- Genetic or biometric data (for the purpose of uniquely identifying an individual)
- Health data
- Sex life or sexual orientation
- Commission of criminal offences or alleged criminal offences

Commercially sensitive data

Commercially sensitive data is defined as:

- Financial, commercial, scientific or technical or other information the unauthorised disclosure of which could reasonably be expected to **result in a material financial loss** to the person or organisation to which the information relates, or could **prejudice the competitive position** of that person on the conduct of his or her profession or business or otherwise in his or her occupation.
- Information whose disclosure could **prejudice the conduct or outcome of contractual or other negotiations** of the person to whom the information relates.

Transfer of restricted data

Any transfer of restricted data to a third party must be carried out securely. As a minimum, paper records should be sent by Royal Mail Special Delivery. Best practice should be that the paper records are delivered by hand by the individual responsible for the transfer (where feasible), directly into the hands of the officer of the third party to whom responsibility for the data has been assigned.

Electronic records should, as a minimum, be encrypted and either sent over a secure connection or put onto an encrypted memory stick and delivered by a trusted courier service. Best practice should be that the records are encrypted and the password provided separately by another means. Again, electronic records on an encrypted CD should preferably be delivered directly by the office responsible for the transfer (where feasible) directly into the hands of the officer in the third party to whom responsibility for the data has been assigned.

Any queries about this Schema should be directed to information-matters@port.ac.uk .

University of Portsmouth University
House Winston Churchill Avenue
Portsmouth PO1 2UP United Kingdom

T: +44 (0) 2392 843195
E: corporate-governance@port,ac,uk W: www.port.ac.uk