



# DATA PROTECTION POLICY

## 2019

# Contents

1.0 Introduction .....	3
1.1 Purpose .....	3
2.0 Policy .....	3
3.0 Auditing.....	7
4.0 Contact Us.....	7

# 1.0 Introduction

The lawful and proper treatment of Personal Data is extremely important to the ESO and key to the success of our business and our ability to maintain the trust and confidence of our employees, students, contractors, suppliers and clients.

Our approach is to ensure full compliance with the relevant sections of the EU General Data Protection Regulation (the “GDPR”) and it is the responsibility of all employees, other workers and students to support the Board of Trustees and Executive Team in maintaining that level of compliance.

## 1.1 Purpose

The purpose of this policy is to establish a number of basic requirements for how the ESO will process personal data to ensure the integrity of the data subjects.

# 2.0 Policy

## 2.1 KEY DEFINITIONS

Data Controller	is the ESO which alone or jointly with others such as the Board of Trustees and/or Executive Team, key managers and employees determines the purposes and means of the processing of personal data
Data Processor	is the employee, worker, student who has responsibility for processing personal data on behalf of the Data Controller
Data Subject(s)	is defined as the identified or identifiable person whose personal data is being processed eg. employee, staff, student, client, applicant
Personal Data	is defined as any information relating to an identified or identifiable person (a “natural person”), including but not limited to names, addresses, e-mail addresses, numbers, dates, photos, images, on-line identifiers, location data, physical, physiological, genetic, biometric, mental, economic, cultural or social identity data. Personal data relating to employment such as work e-mail addresses, phone numbers etc. are included within this definition.
Special categories of personal data	Personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data

Processing of personal data is defined as 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. Processing would include remote viewing of Personal Data.

## 2.2 PROCESSING OF PERSONAL DATA

### 2.2.1 Lawful Bases

There are six lawful bases on which personal data can be processed:

1. Consent: the individual has provided clear consent for us to process their personal data for a specific purpose.
2. Contract: the processing is necessary to fulfil a contract we have with the individual whether that processing is as part of the contract or a necessary step in advance of entering into the contract.
3. Legal obligation: the processing is necessary for us to comply with law.
4. Vital interests: the processing is necessary to protect someone's life
5. Public task: the processing is necessary for us to perform a task in the public interest and/or for official functions and there is a clear basis in law for doing so.
6. Legitimate interests: the processing is necessary for our legitimate interest or those interests of a third party.

We will always process personal data under one of the above lawful bases.

If consent has not been given, special categories of personal data may, in principle, only be processed if it is necessary to exercise employment law rights or obligations or to justify a legal claim.

### 2.2.2 Information to the natural persons about the processing of their personal data

A natural person whose data is to be processed has the right to receive certain information before the processing activity is carried out. Such information will include e.g. the identity of the data controller, the purposes of the processing and the legal basis, any recipients of the personal data and any intention to transfer the data outside the EU/EEA.

At ESO we process personal data relating to a range of natural persons including employees, consultants, students, alumni, clients, as well as job and student applicants and clinic patients.

### 2.2.3 Purpose and limitation of processing

Personal data will only be processed for a specified, explicit and legitimate purpose. Only personal data that is necessary for the specified purpose may be processed. If a purpose changes over time, it will be considered as a new processing activity that requires a legal basis.

Further, personal data will be adequate, relevant, accurate, up to date and limited to what is necessary in relation to the purposes for which it is collected. Therefore, we will also ensure that we

use reliable sources when collecting the data and, where relevant, allow the data subject to update his/her own personal data where possible.

#### 2.2.4 Data Protection Impact Assessment (“DPIA”)

The ESO will undertake a DPIA prior to the processing of any data which has a highly likelihood of impacting the rights and freedoms of any individual.

#### 2.2.5 Internal Records of Processing Activities

To comply with its legal obligations the ESO maintains records of all processing activities. These records are reviewed on a quarterly basis by the respective Data Controller and Data Processor; and submitted to the Executive Team for approval.

### 2.3 STORAGE OF PERSONAL DATA

Personal data will not be processed for a longer period than necessary considering the purposes for which it was collected. The following table provides information of the time limits for retention.

Type of data	Retention period
Employee/staff files	6 years post departure
Job applications (CVs, interview notes, letters/emails)	6 months post application
Speculative enquiries from prospective students	1 year or commencement academic year (whichever sooner)
Student applications (unsuccessful)	6 months post application
Student files	6 years post departure (save for *)
*Academic transcripts and dissertations etc	Indefinitely
Exam Scripts: - University of Greenwich curriculum - Bucks New University curriculum	1 full academic year after year of examination 6 months after exam board ratification
Alumni network	As long as individual remains member of network
Payroll data	3 years post departure
Patient files	
- Adults with no mental health issues	8 years after last interaction
- Children up to 18 years old	Until 18 years old plus 8 years

Consent will always be obtained where it is intended to keep an individual’s personal data longer than the period set out above and the retention period will only be extended where there is a legal basis for doing so.

If a data subject exercises his/her right to be forgotten or withdraws consent, the personal data will be deleted if there is no other legal basis to process it e.g. if there is a legal obligation to retain the personal data, then the personal data will be retained and processed only for that specific purpose.

## 2.4 INTEGRITY & CONFIDENTIALITY

The ESO will implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorised disclosure or access and any other unlawful forms of processing. ESO employees, workers and students must ensure that all personal data is processed in a manner that ensures that it is always secure, confidential and available and will not be unlawfully, accidentally or without authorization disclosed, amended, lost or damaged.

## 2.5 TRANSFERRING DATA OUTSIDE THE ORGANISATION AND/OR THE EU/EEA

When it is necessary for the personal data of our data subjects to be processed by a third party, then we will ensure that we have sight of the third party's Data Protection Policy and confirmation as to whether the data will be transferred outside of the EU/EEA. In these circumstances, we will notify data subjects of the transfer due to the restrictions in place in respect of transferring personal data outside of the EEA. We will always consider these restrictions and put in place the required safeguards and protections.

## 2.6 THE RIGHTS OF DATA SUBJECTS

Data subjects have certain rights, as are further detailed in the applicable data protection legislation and in our Privacy Notices. These rights are:

- a right to access (a record that shows what data is being processed about him/her)
- rectification
- erasure (right to be forgotten)
- restriction of processing
- portability; and
- objection.

If you wish to exercise one or more of the above rights, then please contact the relevant Data Processor. If you feel that the ESO has not complied with your data protection rights, then you can complain to the Information Commissioner's Office.

## 2.7 RESPONSIBILITIES

The Executive Team has overall responsibility for the ESO's compliance with data protection.

Every ESO employee, worker and student is responsible for reading, understanding and following the standards set out in this Policy.

ESO managers are responsible for ensuring that this Policy is implemented within their departments and that the employees and/or staff within their area of responsibility are familiar with and follow the standards set out in this policy

The Executive Team is responsible for the maintenance, training and monitoring of this policy.

All employees, workers and students are required to report to the Executive Team any data privacy related concerns, violations of this policy or suspected data incidents

The ESO will not tolerate any form of harassment, discrimination or retaliation against someone who has raised a concern and acted in good faith in respect of this policy.

## 3.0 Auditing

Policy Name:	Data Protection
Policy Owner:	Head of Quality
Policy Approver:	Policy Management Committee
Audience:	All employees, students, prospective students, alumni, clients
Storage Location:	Learning Zone – Governance; Website
Effective Date:	02.2019
Review Date: (Unless other revisions are required prior to this date)	02.2020
Version:	Approved version 1.0
Equality Impact Assessment:	Are there any implications for a protected characteristic group as defined by the Equality Act 2010 in this policy? <input type="checkbox"/> Positive Impact <input type="checkbox"/> Negative Impact <input checked="" type="checkbox"/> Neutral
Details:	<Provide details if there is a either a positive or negative impact>

## 4.0 Contact Us

### Business Address

Boxley House  
The Street  
Boxley, Maidstone  
Kent ME14 3DZ  
United Kingdom

### Contact Information

Paula Fletcher  
Head of Quality  
T: +44 1622 671558  
E: paulafletcher@eso.ac.uk

### Further Information

If you have further questions regarding this document or require further information, please contact our team.