The General Data Protection Regulation (GDPR) Policy and Procedure For Oxford Education Consulting

1 Introduction

Oxford Education Consulting is an online teaching provider, educational consultancy and student placement agency.

This policy supports the legal requirements of the UK General Data Protection Regulation (GDPRUK), tailored by the amended Data Protection Act 2018, which places certain obligations on the Company, its staff and those who process data on our behalf.
Our clients originate in the UK or outside the EU, but for those that are resident in or are EU nationals the provisions of the EU GDPR still apply

This policy will be reviewed by the officer responsible for Data Protection on an annual basis. It may however be amended in advance of such date in response to changes in future legislation. The next anticipated legislation is the Data Protection and Digital Information Bill (No 2) currently undergoing parliamentary scrutiny and process now.

The school is committed to ensuring that its staff and contracted teachers are aware of data protection policies, legal requirements and briefings and training is provided to them.

2 Organisational Scope

2.1 This GDPR policy is a corporate policy and applies to former, current and potential employees and associates of Oxford Education Consulting (OEC). This policy will form part of an agreements with any organisation processing personal data on behalf of the Company.

2.2 We are a data controller and data are processed by our staff in the UK, However, for the purposes of IT conference hosting and file maintenance some information is located on the cloud to be precise we use Microsoft 365 Sharepoint to store all information. Emails can be encrypted if necessary.

2.3 Data is backed up incrementally on an external hard drive and which is subsequently disconnected from the network and stored in a lockable container in a separate location. We have conducted an information audit and we currently collect and process the following information:

Personal identifiers, contacts, and characteristics i.e., full name, Date of Birth, gender, nationality, visa Biometric Residence Permit, passport and contact details of parents,

students, employees, teachers core staff.

Personal images for identification. Normally taken from a Passport provided by the subject or directly by the subject.

Other files relevant to the provision of our service.

Medical, including allergies and medications.

Cultural data.

Financial, including invoice and pricings and payroll.

Academic data such as school reports, notifications, and disciplinary matters.

Lifestyle such as likes, dislikes, sports, hobbies.

Employee, contractors /consultants vetting and recruiting information.

Proof of Right to Work (RTW) in the UK such as a UK Passport or other documentation such as BRP, Home office letter of indefinite right to remain or a visa vignette.

Proof of Identity and address documentation for DBS processing. Only the RTW document is retained the remainder is deleted after DBS processing is complete.

3. Definitions

This section includes all necessary definitions of terms used in the policy which are not in everyday usage or where there is a need to be precise.

3.1 Consent

Consent means offering people genuine choice and control over how you use their data. Consent must be freely and explicitly given to be valid under GDPR.

3.2 Data Subject

Data subject means “an individual who is the subject of personal data”. A data subject must be a living individual.

3.3 Information Commissioner’s Office (ICO)

The UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO enforce the law regarding information compliance legislation.

The UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO enforce the

law regarding information compliance legislation.

3.4 Lawful Processing for Legitimate Interests
processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3.5 Personal data
means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified,
directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

3.6 Processing of Personal Data
Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.

3.7 Records Disposal
The School will retain records for only as long as they are needed and then, when they are no longer needed, destroy them in an appropriate manner or dispose of them in some other way, e.g., by transfer to an archives service.

3.8 Retention period
The periods of time, varying from a few months to permanency, during which a record has to be maintained by the Company. This is usually determined by statute, legal, regulatory or business compliance, or where these do not apply, by a best assessment of risks involved in destruction against the costs of retention. E.g., The right to work in the UK documents are held for two years after the cessation of employment but accounting records are held for 6 years.

3.9 We are obliged to see the original DBS certificates to confirm the applicants' details, the clearance is enhanced, the certificate number and date of issue and that the children's barred list has been checked. We do not keep a copy but record the details as described on the School Single Central Record and a separate record of those details and the DBS certificate number and the date issued. When checking the currency of an associate enrolled on the DBS update service we conduct an 'employers' check using Name, Certificate number and DOB at https://secure.crbonline.gov.uk/crsc/check?execution=e1s1

3.10 School Community
For the purposes of this Policy this includes core staff, students, contractors, teachers and others with a direct impact on or responsibility to the Company

4. Policy Statement

The School and individual members of the School community are expected to abide by the laws in force in this area. All School staff and contractors processing data on behalf of the School are responsible for any breaches of such legislation.

5. Key Principles

5.1 OEC is strongly committed to complying with its legal obligations regarding the protection of personal data and privacy of individuals.

5.2 This Policy and procedure sets out the minimum requirements for data processing by the School so as to protect the rights of data subjects.

5.3 OEC needs to keep and process certain information about its employees, contractors, students and others to allow it to comply with legal obligations, and to operate in an effective and efficient manner.

5.4 To comply with the existing Data Protection Act requirements and the General Data Protection Regulation, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, OEC staff, students and contractors must comply with the Principles and protections set out in the Data Protection Act currently in force, GDPR 2018 and reiterated in the OEC GDPR Policy.

5.5 The OEC must only retain personal data in line with the guidance set out in the OEC Retention Schedule. This document provides advice as to retention periods suitable for types of records prior to any disposal decisions being made.

5.6 All processing of personal data under the GDPR needs to have a legal basis, and the OEC must be able to demonstrate, to the ICO or to the individual, this basis using logged documentation.

5.7 It is important to determine the legal basis for processing as under the GDPR this has an influence on an individual's rights. For example, consent provides individuals with stronger rights such as having data deleted.

5.8 Processing Conditions are:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- 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 controller
- Processing is necessary for the purposes of the legitimate interests of the OEC or the legitimate interests of a third party.

5.9 The GDPR introduces a duty on the OEC to report serious data breaches to the Information Commissioner's Office, and often to the individuals affected. A notifiable breach has to be reported to the ICO within 72 hours of the OEC becoming aware of it as well as, when appropriate, notification to the data subject within the same tight timescale.

5.10 Fines have increased and the maximum fines can be up to 20 million Euros or 4% global turnover for a breach, depending on the severity, scale or impact of the breach. For example, the loss of hundreds of minor pieces of personal information might incur a smaller fine than a case where the OEC loses the sensitive personal health information of one individual.

5.10 Failure to report a breach can also result in fines for the OEC and potentially for the individual who has committed the breach. OEC requires all incidents and breaches to be reported to the Officer responsible for GDPR so we can assess and reduce the risks and where possible prevent incidents from becoming serious breaches.

5.11 All employees and contracted teachers are briefed on induction and must undertake the GDPR e-learning or provide proof of having done so.

6. Procedure

6.1 Data Held and Processed by OEC

a. OEC will use and otherwise process records of personal information relating to data subjects relevant to the effective functions and operation of its role as an online education provider and employer.

b. Where required, The OEC will obtain freely given consent for all types of personal data processing except that specifically exempted by the Regulation.

c. The use of the information and retention of the personal data will be specifically defined within the OEC central personal data processing log.

d. All staff, contractors, students and other data subjects about whom personal information is held may have the following rights:

- The right to be informed
- The right of access

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

e. Some of these rights may be restricted depending on the lawful basis the OEC is relying on for the processing and can also affect which rights are available to individuals. The ICO provides the following examples:

	Right to erasure	Right to portability	Right to object
Consent	✓	✓	X but right to withdraw consent
Contract	✓	✓	X
Legal obligation	X	X	X
Vital interests	✓	X	X
Legitimate interests	✓	X	✓

These rights are explained further in Appendix A

f. This adds to the existing rights previously in place for data subjects which include a person's right to know:

- what information OEC holds and processes about them
- why the information is held and processed
- details of whom the information might be shared with
- know how to gain access to such information
- know that it is up to date
- know what OEC is doing to comply with its obligations under the Data Protection Act or other relevant legislation

7. Responsibilities of Staff in Relation to their own Data

7.1 All core staff, teachers or consultants are responsible for:

Checking that any personal data that they provide to the OEC is accurate and up to date: they are requested to check this periodically informing OEC of any changes or errors in the information held.

8. Responsibilities of Students in Relation to their own Data

8.1 Parents, legal guardians and students over the age of 13 will, at the time of registration, be required to agree to the use of essential personal data for OEC administrative purposes, which will be clearly specified.

8.2 Parents, legal guardians and students must assist OEC in ensuring the accuracy of the personal data as provided to the OEC and that the information is up to date.

9 Basic responsibilities on staff for Data Security of Third Party Personal data

9.1 OEC has a legal requirement to ensure that data is held securely and this includes the provision that access and disclosure of personal data should be restricted to those who have a legitimate, authorised purpose.

9.2 Staff and consultants /teachers have a responsibility for using and otherwise processing personal data in compliance with this Policy and more specifically operating under the terms of the relevant Data Protection legislation.

9.3 Therefore, all OEC staff and associates are responsible for ensuring that:

a. personal information is not disclosed by them either orally or in writing, to any unauthorised third party
b. they do not access any personal data which is not necessary for carrying out their work/teaching
c. personal data in paper format is kept in a secure place when not being processed

10 Responsibilities on students for Data Security of Third Party Personal data

10.1 Students and teachers may need to process personal information for lesson projects or surveys but the data subject should be informed of details such as why the data is being collected and how long it will be retained for.

11 Right of Access to Information

11.1 The ICO provides information regarding valid requests for a data subject to access their personal data (A Subject Access Request).

- it should be made in writing.
- A request sent by email or fax (and potentially via social media) is as valid as one sent in hard copy.

- If a request does not mention the Act specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data. The GDPR provides for a data subject to have the right of erasure of personal data.

12 Right to Erasure

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances, which are:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent (if consent has provided the justification for processing).

12.1 All data subjects have the right to apply for access to any personal data that is being kept by about them either digitally or on paper files. Any person who wishes to exercise this right should make a written request to the officer responsible for data protection (Sarah Bacon). OEC cannot charge any fee or disbursement for such a service

12.2 All requesters will be asked to include proof of identity and no response will be sent until such proofs have been provided. The OEC will ensure that requests for information are responded to within the statutory month period.

13 Right to Data Portability

13.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

13.2 It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

However, the right to data portability only applies:

13.3 to personal data an individual has provided to OEC.

13.4 where the processing is based on the individual's consent or for the performance of a contract; and

13.5 when processing is carried out by automated means.

14 Right to Object

Individuals have the right to object to:

- processing based on legitimate interests (including profiling).
- Data used for unauthorised marketing purposes
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e., in breach of the GDPR).
- The personal data must be erased in order to comply with a legal obligation.

14.2 Individuals must have an objection on "grounds relating to his or her particular situation". Therefore, OEC will have to stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

15 Publication of OEC Information

There may be Information that is already in the public domain, for example OEC web pages.

16 Personal Data Breach

16.1 All personal data breaches should be reported to the responsible officer and relevant line management who will make a judgement on the severity of the breach.

16.2 Breaches involving large losses or misuses of personal data or any involving 'sensitive' personal data will be reported to the responsible officer to investigate more fully. To help assess the seriousness of a breach please refer to Appendix 2 and Appendix 3.

16.3 Data breaches may include hacking by external actors or misuse of OEC officer or remote working computers .

16.4 In the event of a theft of data or a company device containing data when away from the OEC, the police should also be notified of the theft.

17 Actions to be taken in Response to a Personal Data Breach

17.1 As soon as a breach has been detected or is suspected the following steps should be taken:

17.1.1 An immediate attempt should be made by the line manager or Co- Ordinator to recover any personal data lost or misplaced.

17.1.2 Liaise with those involved with the Breach to prevent the further worsening of any breach.

17.1.3 Consideration should be given as to whether to notify those affected by any such Breach. The OEC is strongly in favour of notifying those affected but in any event those who may suffer damage (including reputational damage) or loss should always be informed.

17.1.4 Steps should be taken to review processes and procedures to reduce the risk of further breaches happening again.

17.1.5 Systems and procedures will be reviewed by the responsible Officer 3 months after the breach to make sure processes have been made more robust.

17.1.6 Where relevant, those affected should be informed of the steps that have been taken to recover their personal data and reviews that have started to prevent issues happening in the future.

17.1.7 Staff or associates responsible for major breaches or repeat minor breaches will be required to undertake remedial Data Protection training.

17.1.8 In the case of serious Breaches, deliberate breaches or repeated breaches after training, The OEC Director will review the employment status of the individual concerned

17.1.9 In the case of serious breaches, the OEC Officer responsible for data protection will be legally obliged to report such a breach to the Information Commissioner's Officer. This may result in fines for the OEC and for those committing major breaches.

17.1.10 The Data Protection Officer will retain records for all serious breaches.

18. Notification:

18.1 Our data processing activity is registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO at:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

18.2 Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

18.3 OEC employees or associates who discover a data breach must report this immediately to the responsible staff member, Sarah Bacon, who will investigate to discover the extent and severity of the data loss.

18.4 Breaches of personal or sensitive data shall be notified immediately to the individual(s) concerned and if significant within 72 hours to the ICO.

19. Data Disposal

19.1 The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. Long term data is held on the cloud via Microsoft 365 Sharepoint. Temporary Data such as recruiting and application data held on devices are permanently and irretrievably deleted after immediate use. School issued devices have 'File Shredder 'installed which will delete irretrievably. Sensitive data held on other devices such as contract teacher's personal PC must also be deleted. The school recommend three free apps. They are: File Shredder, Eraser, and Freeraser

19.2 Time expired devices, thumb drives, CDs, tape, or other electronics no longer required shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. Paper records, if any, will be destroyed by fire on school central office property by the officer responsible for Data Protection.

19.3 Disposal of IT assets holding data shall follow ICO guidance: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

20. How to complain

In the first instance data subjects should contact Sarah Bacon by email at sarah@oxfordeducationconsulting.com or by telephone at **+44(0)1604859331**. Or by Post to**, Oxford Education Consulting, The HIF, Gayton, Northamptonshire, NN7 3EY** You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113

References

The General Data Protection Regulation 2018

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Data Protection Act 2018

Privacy and Electronic Communications Regulation

Information Commissioner's Office Overview of the General Data Protection Regulation (GDPR)

Information Commissioner's Office Privacy Notices, Transparency and Control – a code of practice on communicating privacy information to individuals

Information Commissioner's guide to data protection

Information Commissioner's Office GDPR Consent Guidance (Currently in consultation)

Information Commissioner's Office Guide to Privacy and Electronic Communications Regulation

Freedom of Information Act 2000

Version Control

Record of Amendments		
Date	Details of Change	Name
9 July 2022	Introduction of student placement and Online teaching platform into OEC description More clarification of the key principles and lawful basis for processing in light of ICO guidance and the GDPR	KT Bacon
30 July 2023	Introduction of imminent legislation. Data Protection and Digital Information Bill (No 2) currently undergoing parliamentary scrutiny and process now.	SA Bacon

Reviewed By	date	Peer Review by	
KT Bacon	19/12/2020	SA Bacon	22/12/2020
KT Bacon	15/07/2021	SA Bacon	28/07/2021
KT Bacon	09/07/2022	SA Bacon	18/07/2022
SA Bacon	30/07/2023	KT Bacon	30/07/2023

Appendix 1 EXAMPLES OF INCIDENTS WHICH SHOULD BE INVESTIGATED

This will not be a complete list but is designed to provide advice as to potential breaches that may occur.

- Sending emails or correspondence containing personal data to the wrong recipient.

- Sending non-essential personal data to otherwise valid recipients (for example including a string containing health details to all recipients when only one has rights to see it).

- Personal data received in error.

- Failure to secure access to OEC devices, including incorrect allocation of permissions or sharing passwords, which result in unauthorised access to personal data.

- Misuse of OEC computer systems to access personal details where there is no business purpose to do so

- Loss or theft of any OEC-owned data storage device regardless of the data it contains e.g., laptop, PC, USB/pen drive, iPad or other tablet, removable

APPENDIX 2 Guidance to Data Protection Co-Ordinators on Assessing Breaches.

This is intended as a guide only and not all specific circumstances may be included in the table – If in doubt please contact the officer responsible for data protection for additional advice and support.

No. of individuals whose datahas been disclosed or otherwise putat risk	1. Very Minor Incident	2. Minor Incident	3. Serious Incident	4. Major incident
) with one or more of the following characteristics : • No sensitive personal data • Information already accessible or in public domain • Low level of harm to individuals				
Plus, following characteristics: • No sensitive personal data involved • Information already accessible or in public domain • Low level of harm to individuals				

with one of the following characteristics : • One or more previous similar incidents in last 12 months • Failure to implement, enforce or follow technical safeguards to protect information				

plus, with one or more of the following characteristics : • Several previous similar incidents in last 12 months • Failure to implement, enforce or follow technical safeguards to protect information				

with one of the following characteristics: • Detailed information at risk e.g. clinical care case notes, social care notes • High risk confidential information • Likely to attract media interest or other reputational damage and/or a complaint has been made to the ICO by an organisation or individual • Individuals are likely to suffer substantial damage or distress including significant embarrassment or detriment • Individuals likely to have been placed at risk of incurred physical harm				
with more than one of the following characteristics: • Detailed				

information at risk • High risk confidential information • Likely to attract media interest or other reputational damage and/or a complaint has been made to the ICO by an organisation or individual • Individuals are likely to suffer substantial damage or distress including significant embarrassment or detriment • Individuals likely to have been placed at risk of incurred physical harm				

Appendix 3 Points for Investigating Staff to Consider

- What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)
- How did the breach occur?
- What type of Data is involved? (The individual data fields should be identified e.g. name, address, bank account number)
- How many individuals or records are involved?
- If the breach involved personal data, who are the individuals?
- What has happened to the data?
- Establish a timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)
- Were there any protections in place? (e.g. Encryption)
- What are the potential adverse consequences for individuals or OEC? How serious or substantial are they and how likely are they to occur?
- What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?
- What processes/systems are affected and how? (e.g. web page taken offline, access to database restricted)

APPENDIX 4: Breach Log Template

Completed forms to be retained by DPO

Questions	Answers
When did this Breach occur? When was it reported?	
What are the personal data affected?	
How many people will have been affected?	
Where are the data now and how many people with no rights to access it have seen it?	
What has been done to recover the data?	
What policies or procedures have been put in place or amended to stop a recurrence of this Breach?	
What training/ awareness raising measures have been taken in the light of this Breach?	

Has this happened before?	