Data Protection Policy

Policy no:	8.10
Version no. & date:	V0.8
Next review due:	September 2023
Responsible Committee/Person:	Compliance Committee and Data Controller
Approved by & date:	SMT October 2020
Linked policies:	8.5 Data Privacy Notice and Consent Policy 8.6 Policy on your Rights in Relation to your Data
External references	Data Protection Act 1998, 2018 Article 51 GDPR
	UK Quality Code UKSCQA/02 Advice and Guidance on Monitoring and Evaluation (6.7) *Providers take account of ethics and data protection requirements when designing and operating monitoring and evaluation systems.*
	ICO No. Z1097339
	optindigo.com for GDPR Consultancy and Support
Audience:	Internal and External Stakeholders (Website, face to face, email, College notice boards)

Contents

1 Introduction

The College is committed to a policy of protecting the rights and privacy of individuals to include students, staff, other stakeholders and members of the public. This policy sets out how the College will meet its obligations under the Data Protection Act 1998, 2018, and Article 51 of the EU GDPR and will ensure that the College is aware of and proactively protects against risk of data breaches to individuals whose data is paced under our care including students, staff, Board of Governors and all other stakeholders. This policy should be read in conjunction with the College's polices: 8.5 *Data Privacy Notice and Consent Policy* and 8.6 *Policy on your Rights in Relation to your Data.*

2 Purpose

The College needs to process certain information about its students, staff and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. This policy sets out how the College aims to protect the data it is required to process and store.

3 Scope

The policy applies to all staff and students at the College. Any breach of the Data Protection Act 1998 or the College Data Protection Policy is considered to be an offence and in that event, Oxford Business College disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the College, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

4 Staff

There are clear legal and business reasons for keeping data about students and employees. However, under the Data Protection Act 1998, the Academy also has important legal duties relating to maintenance of staff records and what it does with them.

Employees are entitled to access certain records and can seek compensation for damage or distress suffered as a result of a breach of the Act. This means that all managers should take care when recording information about their staff.

This policy explains what staff records should be kept and for how long and offers advice and explains the College's legal obligations as an employer and employees' rights regarding information held about them.

4.1 Keeping staff records: the legal requirements

To comply with the law, the College should keep records on:

- hours worked, and employees who have agreed to work more than 48 hours, to meet the requirements of the Working Time Regulations
- pay rates; to meet the statutory requirement to issue employees with pay statements and to ensure that the requirements of the National Minimum Wage Act 1998 are met
- payroll: i.e. on income tax and National Insurance deductions, for HM Revenue & Customs
- sickness of more than four days and how much statutory sick pay has been paid
- accidents, injuries and dangerous occurrences - to meet health and safety requirements

- accounting data
- crime prevention information
- pensions data

4.2 Other staff records that should be kept:

Records of each employee`s:

- training and appraisals
- employment history - date employment began, promotions, job title(s)
- absence - records of lateness, sickness, and any other authorised or unauthorised absences
- personal details - name, address, emergency phone number(s), qualifications, work-relevant disability
- terms and conditions and employment - including a copy of each employee's written and correspondence relating to any changes to their terms and conditions

More general records:

- meetings with workplace representatives
- any disciplinary action taken, and records of disciplinary hearings
- individual and collective redundancy consultation meetings and agreements
- negotiations relating to information and consultation agreements

4.3 The level of detail in employee records

According to the principles of the Data Protection Act 1998, any personal information kept on employees should be adequate, relevant and not excessive. Inadequate records lead to problems when dealing with absence levels, staff turnover, sickness, lateness and discipline. The records system should be simple, reliable and flexible.

Not all records can be maintained electronically; employee files will also need to hold signed copies of certain key documents; this is especially important in the event of any tribunal claims against the College. Good practice in data security includes:

- a lockable paper filing system
- access to the data only granted to staff who need to use it
- electronic records protected with passwords, anti-virus software and firewalls
- an audit trail used with computerised systems to enable checks on who has accessed a particular record and when

4.4 How long to retain staff records?

It is good practice to retain records for six years, to cover the time limit for bringing any civil legal action against the Academy, including national minimum wage claims and contractual claims.
The following table gives more specific guidance for particular types of records.

4.5 Record Statutory retention period

Documents/Data	Retention Period
Accident reports	Three years after date of last entry. There are rules on recording incidents involving hazardous substances
Payroll records	At least three years after the end of the tax year they relate to
Statutory maternity, adoption and paternity pay records	Three years after the end of the tax year they relate to
Statutory sick pay records	Three years after the end of the tax year they relate to
Working time	Two years from date on which they were made
National minimum wage records	Three years after the end of the pay reference period following the one that the records cover
Retirement benefits schemes - notifiable events, e.g., relating to incapacity	Six years from the end of the scheme year in which the event took place

4.6 Record Recommended retention period

Documents/Data	Retention Period
Application forms/interview notes for unsuccessful candidates	One year
Health and safety records of consultations	Permanently
Parental leave taken	Five years from birth/adoption, or until child is 18 if disabled
Pensioners' records	12 years after benefit ceases
Disciplinary, working time and training records	Six years after employment ceases
Redundancy details	Six years from date of redundancy
Senior executives' records	Permanently for historical purposes
Trade union agreements	Ten years after ceasing to be effective
Minutes of trustee/work council meetings	Permanently
'Right to work' documents	Two years after employment ceases

The Data Protection Act 1998 states that data should not be retained any longer than is necessary for a particular purpose. When data is no longer required it should be disposed of securely and effectively, e.g., by shredding. Where possible, data on employees and former employees should be made anonymous before disposal.

5 Requirements of the Data Protection Act

The Data Protection Act 1998 is concerned with personal data - information about living, identifiable individuals held on computer or in certain structured manual filing systems. There are eight clear principles for processing such data to comply with the Act.

Data should be:

- processed fairly and lawfully - make sure employees understand why you are collecting the data and how you will use it for specified and lawful purposes - beware of using information obtained for one purpose for a different purpose or passing on personal information to third parties when you are not sure that they are entitled to it
- adequate, relevant and not excessive
- accurate and, where necessary, kept up to date
- kept no longer than necessary
- processed in line with individuals' rights, including their right to access
- kept secure with appropriate technical and organisational measures taken to protect the information
- prevented from being transferred to countries outside the European Economic Area unless there is adequate protection for personal data

These principles should be considered when deciding what information to collect, when establishing procedures for processing this information and when dealing with requests from employees. Failure to comply with the Act and the data protection principles could result in the Information Commissioner's Office (ICO) issuing an enforcement notice. Contravention of a notice is a criminal offence. Staff and other individuals can also seek compensation if they suffer damage (usually physical or financial) or distress as a result of a breach of the Data Protection Act 1998 by the business.

6 Notifying the Information Commissioner`s Office

In addition to complying with the Act and the data protection principles, the College Data Controller is expected to notify the ICO about processing of personal information (unless exempt). The ICO issues guidance on this process and on how to comply with data protection legislation. Failure to notify the ICO (unless exempt) is a criminal offence.

7 Employees` rights of access to data

Under the Data Protection Act 1998, individuals have a number of rights, in particular the right to access any information held about them. If an employee asks for any information held about them - a subject access request - they must make the request in writing, The Academy is permitted to charge up to £10 for providing the information and should reply within 40 calendar days.

Information that the Academy is not required to provide under subject access requests:

- information held for management planning, e.g., plans to promote an employee or make an employee redundant
- information as to your intentions in respect of negotiations with the requester
- references you have given about the worker in confidence (references received by you are not exempt)
- information about the prevention or detection of a crime, or the arrest or prosecution of offenders
- information that may identify someone else

As well as the right to access data on themselves, an employee also has the right to:

- have inaccurate personal data corrected
- compensation for damage suffered as a result of any breach of the Act
- prevent processing likely to cause substantial damage or substantial distress
- be told the rationale for any automated decision taken about them, e.g., psychometric testing decisions

If an employee has reasonable grounds to believe you have not paid them the national minimum wage, they have the right to see their pay records. They must make a written request, and the records must be produced within 14 days.

8 Additional guidance on Data Protection issues

Acas helpline
08457 47 47 47
National Minimum Wage helpline
0845 6000 678
Information Commissioner's Office Data Protection helpline
01625 545 745
Health & Safety Executive Infoline
0845 345 0055
Information Commissioner's Office Notification Line
01625 545 740

9 Responsibilities under the Data Protection Act

Compliance with data protection legislation is the responsibility of all members of the College who process personal information. Staff of the College are responsible for ensuring that any personal data supplied to the College are accurate and up to date.

10 Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The College understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by the College (e.g. when a student signs a registration form or when a new member of staff signs a contract of employment). Any College forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.

If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any member of the College is in any doubt about these matters, they should consult the College Data Controller or refer matter to the Compliance Committee chaired by the Executive Principal.

11 Disclosure of Data

The College must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of College business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the College concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

- The individual has given their consent (e.g., a student/member of staff has consented to the College corresponding with a named third party);
- Where the disclosure is in the legitimate interests of the institution (e.g., disclosure to staff - personal information can be disclosed to other College employees if it is clear that those members of staff require the information to enable them to perform their jobs);
- Where the institution is legally obliged to disclose the data (e.g., HESA and HESES returns, SLC, HEFCE, ethnic minority and disability monitoring);
- Where disclosure of data is required for the performance of a contract (e.g., informing a student's or sponsor of course changes/withdrawal etc).

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security*;
- Prevention or detection of crime including the apprehension or prosecution of offenders*;
- Assessment or collection of tax duty*;
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)*;
- To prevent serious harm to a third party;
- To protect the vital interests of the individual, this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member of the College, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the College may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the College may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer;
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the College" to avoid confirming their membership of their presence in or their absence from the institution.

Further information regarding the disclosure of personal information can be found in Appendices V (student information) and VI (telephone protocol).

If in doubt, staff should seek advice from their Line Manager or Campus Principal.

12 Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding or secure electronic deletion).

13 Use of CCTV

The College's use of CCTV is regulated by a separate Code of Practice.

For reasons of personal security and to protect College premises and the property of staff and students, close circuit television cameras are in operation. This policy determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out only by a limited number of specified staff;
- The recordings will be accessed only by the IT manager, HR manager or a director;
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

14 Informing Students of Disclosures and Obtaining Consent

Students should be informed of predictable disclosures (such as confirmation of student status, responding to a request for a reference) when they register with the College. Some students will choose to opt out of certain processing (including disclosures) on their registration form. This information is recorded on the College database and all staff should check a student's record before releasing any information.

- In less predictable situations (e.g. family member phoning for financial details, taxi firm who has found wallet and wants to contact student) where the student has not been previously informed of a possible disclosure, the student should give their consent before any information is released.
- The College understands "consent" to mean that the student has signified their agreement whilst being in a fit state of mind to do so and without pressure being exerted upon them. There must be some active communication between the parties, consent cannot be inferred from non-response to a communication. In most cases, verbal consent should be acceptable as long as proper security checks are made to ensure that the person giving the consent is the student. For telephone consent, this will mean asking the subject to confirm several separate facts that should be privy only to them (student number, date of birth etc).
- There are certain exemptions (Section 29) from the requirement to inform students of disclosures if the information is being released for the prevention or detection of crime AND if informing the student of the disclosure would prejudice the enquiries. See Section 2 for further detail.

15 Method of Disclosure

- Disclosures should not be made over the telephone. The minimum-security option is to take a number and ring the enquirer back. However, it is strongly advised that all enquirers should be asked to submit their requests in writing (where appropriate on headed paper). Once you have checked whether the request is legitimate or not, you should, wherever possible, reply in writing.

15.1 Disclosure to Work Colleagues

- You should always think carefully before disclosing students' personal information to work colleagues whether they be from within, or external to, your own department. Under the Data Protection Act, you should not disclose personal data to colleagues unless they have a legitimate interest in the data concerned. As there is no definition as to what a "legitimate interest" is, it will have to be a matter of judgment in each case. As a rule you should consider whether or not the information is necessary to allow your colleague to perform their job. So for instance, it would be legitimate to pass information to the Graduation Committee regarding student addresses, degree classification and disabilities if special arrangements were needed to enable the student to attend the ceremony. It would be legitimate to pass the information to the course tutors if extra care is needed in terms of teaching or seating arrangements etc.
- When sharing information with colleagues, you should consider the level of detail necessary to enable them to perform their job. So for instance, if you knew that a student was going to be absent for a significant period of time, you may wish to notify colleagues in the department of this fact. However, it might not be appropriate for all colleagues to be made aware of the specific reasons (health or otherwise) resulting in the absence.

15.2 Disclosure to Relatives/Guardians and Friends

- The College has no responsibility or obligation to disclose any personal information relating to students to relatives, even if they are contributing to tuition fees.

- All students are given the opportunity, both at initial registration and re-registration to provide a data release password. The student may then provide that password to a third party and tell them to quote it whenever they contact the College about them.
- You should always check a student's record to see whether or not the third party is quoting the password held on record. You may come under pressure to discuss individual students with parents/guardians or even friends. However, in these situations it is essential that you do not disclose personal data without the prior consent of the student - it would be a breach of the Data Protection Act to do so. If the student has provided their password to a third party (see above) they are understood to have given prior consent.
- You are, of course, free to discuss institutional procedures with parents (e.g., describing reassessment procedures, releasing dates of graduation ceremonies, advising on when invoices should be paid by), but the specific circumstances of an individual student cannot be discussed without the consent of that student.
- There may be occasional, exceptional circumstances (in which a student's life or health is threatened) in which the usual need to get consent before disclosing to parents/guardians may be waived. The College holds details of students' "next of kin" for such purposes.

15.3 Confirmation of Student Status and Award

- Student status is regarded as personal data and therefore must be processed in accordance with the Data Protection Act, this includes protecting the information against unauthorised disclosure. By confirming whether or not an individual is (or has been) registered at the College could be a breach of the Act.
- The College receives enquiries regarding individuals' student status on a regular basis. The nature of the third party requiring the information can range from current or prospective employers genuinely trying to confirm details on a job application form to estranged or abusive partners trying to trace an individual's whereabouts. Therefore, whenever faced with a request for confirmation of student status, you should exercise caution before responding. The majority of requests will be from agencies with a genuine interest in the information. For this reason, students are informed (on their registration form) that, if requested, details of their student status and final award, will be disclosed to the Home Office, the Police and prospective/current employers/educational institutions. Students are given an opportunity to opt out of these disclosures and so you should always check the student's record before responding. You should always employ appropriate security measures to check the identity of the enquirer and you should not disclose the information over the telephone. Wherever possible, ask the enquirer to put their request in writing, preferably on headed paper.
- For other enquirers, where there is no statutory or other legal obligation for you to disclose information, you should not confirm or deny the student status of an individual without their consent.
- Disclosure to Sponsors (includes Student Loan Company and Research Councils)
- Students are informed that details of their attendance and progression may be passed to sponsors on their registration form and are given an opportunity to object to such disclosures. Before releasing information to a sponsor, you must check the student's record to make sure that they have not opted out of the processing.

15.4 Disclosure to the Student Loan Company

The Student Loan Company (SLC) assesses undergraduate student eligibility for student loan payments. The first assessment is conducted between the student and the SLC and the College would not be involved at this stage. However, the SLC requires confirmation of students' registration status and their attendance on a course. The College is under a statutory obligation to make such disclosures and students are informed of this when they register. Disclosures to SLC should be limited to the facts. Student consent is required if sensitive data (e.g. regarding health) is to be disclosed to their SLC. Where students access SLC funding through one of the College's partner awarding organisations such as a university of college, we will make relevant disclosures to the partner organisation, and they will pass this on to the SLC.

15.5 Disclosure to current and prospective Employers and Educational Institutions

You may receive requests for information regarding individual students (current or former) from current/prospective employers/educational institutions. Typically this occurs when the student has applied for a job or a place on a programme of study. The disclosure will usually be in the best interests of the student and more often than not, the student will be aware that such a request would be made. The information released should be kept to a minimum - usually registration status and/or award. As disclosures of this nature are a regular occurrence, students are informed on their registration form and given the opportunity to opt out. Before releasing the information, you should check the student's record to make sure they have not opted out of this processing. As always, care must be exercised in the method of disclosure.

15.6 Requests for Personal References

- If you receive a request for a personal reference relating to a student, you should ensure that
- The information contained in the reference is FACTUALLY correct
- Where possible, keep the disclosure to a minimum (student's dates of study, marks and/or degree class, registration status)
- Sensitive data (e.g. Details of health to explain absences from the College) must not be disclosed without the explicit consent of the student
- Where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds
- If you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference and thus disclosing personal data
- You do not disclose any information if asked to give an unsolicited reference (for a student who has not, to your knowledge, cited your name as a referee)

The identity of the person requesting the reference should always be confirmed prior to disclosure. Requests for references should usually be made in writing on headed paper. If you receive an email request for a reference, you should be assured that it is a valid request. If it is from a known source or company domain, you should process the request, but you may wish to reply in written format to a known postal address for the company/organisation. If the email domain is not familiar, you are advised to investigate further.

Telephone references are not usually recommended. However, they are acceptable if the student has specifically asked you to provide a reference at short notice. As a minimum security measure it is recommended to ring the enquirer back to check that they are who they claim to be.

Students are informed, on the registration form that we will confirm student status and degree award to prospective employers. Students are, of course, given the opportunity to opt out of this and if they do so, it will be recorded on their student record. The Student Handbook also informs students that we archive student records after graduation, in order to confirm requests from prospective employers, provide references and to provide awarding bodies with evidence of assessed work at a later date. The period of time that records are held depends upon the regulations of our partner organisations and the awarding bodies we work with. The period may range from 3 to 6 years. Whilst it is not guaranteed, it is likely that the College will hold on to records for more than 6 years so that we are able to respond to the needs of our alumni in future if necessary. If a student wishes to replace a lost or damaged certificate, they may do so by contacted the awarding organisation that the College works with. This may be a university, college or awarding body such as Pearson (Edexcel online).

If a student cites a staff member's name as a referee, it is understood that they are giving consent for them to disclose information (regardless of whether they have opted out on their registration form). If the staff member is not aware that a student has cited them as a referee, they should check the validity of the request.

15.7 Disclosures to the Police

Disclosures to the Police are NOT compulsory except in cases where the College is served with a Court Order requiring information. However, Section 29 of the Data Protection Act 1998 does allow limited exemptions from the first Principle meaning that the College may release information to the Police without the consent of students in limited circumstances. Such disclosures should only be made if the Police confirm that they wish to contact a named individual about a specific criminal investigation and where the College believes that failure to release the information would prejudice the investigation. Staff must not release information to the Police over the telephone. The Police must inform the College in writing. Most Police Forces will have their own request form which should always include a statement confirming that the information requested is required for the purposes covered in Section 29, a brief outline of the nature of the investigation, the student's role in that investigation, and the signature of the investigating officer.

15.8 Legal Proceedings

Section 35(2) of the 1998 Act exempts data from the non-disclosure provisions (e.g., obtaining consent from student) in cases where disclosure is necessary "for the purpose of, or in connection with, legal proceedings…..or for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights". In practice this means that the College can disclose information regarding students to its own solicitors when seeking proper legal advice about a case. However, for cases that do not directly involve the University, information should only be disclosed if the relevant student's permission can be obtained. If the information is vital to a case, a Court Order may be issued demanding the information. Section 35(1) specifically allows data controllers to disclose without consent from the data subject (student) when confronted with a Court Order.