Data Protection Policy

Policy no:	6.0
Version no.	24.11
Next review due:	September 2025
Last review date:	November 2024
Responsible Board:	Corporate Planning Board
Approved by & date:	SLT September 2024
Linked policies and documents:	Data Privacy Notice and Consent Policy Policy on your Rights in Relation to your Data
External references	Data Protection Act 2018, 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
Audience:	Internal and External Stakeholders (Website, face to face, email, College notice boards)

Table of Contents

1 Introduction

The College needs to process certain information about its students, staff and other individuals it has dealings with. To comply with the law, the college will ensure that good data protection practice is embedded in the culture of our staff and our organisation). 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.

2 Purpose

The College is committed to a policy of protecting individuals' rights and privacy, including students, staff, other stakeholders and members of the public.

This policy sets out how the College will meet its obligations under the Data Protection Law. It will ensure that the College is aware of and proactively protects against the risk of data breaches to individuals whose data is placed under our care, including all stakeholders. This policy should be read in conjunction with the College's other polices Risk Management Procedure, Data Retention & Deletion Policy, Communication's Policy and Supplier Due Diligence Procedure and Policy on Individual's Rights in Relation to Individual's Data.

'Data Protection Law' includes the General Data Protection Regulation 2016/679, the UK Data Protection Act 2018, and all relevant EU and UK data protection legislation.

3 Scope

The policy applies to all personal data processed by the College and is part of the College's approach to compliance with Data Protection Law. Any breach of the Data Protection Law or the College Data Protection Policy is an offence, and, in that event, Oxford Business College disciplinary procedures will apply. In addition to college staff, all partners, third parties, 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 Aims and Objectives

4.1 The aims of this policy are to:

4.1.1 Ensure the College adheres to applicable data protection regulations, industry standards, and best practices in handling personal data.

4.1.2 Promote a culture of data protection and privacy awareness within the organisation, fostering responsible and ethical handling of personal data.

4.1.3 Maintain transparency, fairness, and accountability in all data processing activities, respecting the rights and privacy of individuals whose data is processed by the organisation.

4.1.4 Implement robust and secure data processing systems and practices, safeguarding personal data from unauthorised access, loss, or damage.

4.2 The objectives of the policy are:

4.2.1 To ensure the College adheres to applicable data protection regulations, industry standards, and best practices in handling personal data.

4.2.2 Promote a culture of data protection and privacy awareness within the organisation, fostering responsible and ethical handling of personal data.

4.2.3 Maintain transparency, fairness, and accountability in all data processing activities, respecting the rights and privacy of individuals whose data is processed by the organisation.

4.2.4 To implement robust and secure data processing systems and practices, safeguarding personal data from unauthorised access, loss, or damage.

5 Responsibilities

The College is both a data controller and a data processor under the GDPR/DPA 2018.

5.1 All line managers are responsible for ensuring personal data is handled in accordance with the College's policies and procedures and for encouraging best practices in the handling of personal data:

5.1.1 The DPO [Bulletproof Cyber Ltd, atousa.vaziri@bulletproof.co.uk] and Chief Operating Officer are accountable to the Board of Governors and for ensuring compliance with data protection law can be demonstrated.

5.1.2 Compliance with data protection law is the responsibility of all employees, partners and third parties working on behalf of the College.

5.1.3 The Managing Director is ultimately accountable for ensuring the college is compliant with data protection law.

5.1.4 The College will ensure that all staff, partners or third parties who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

5.1.5 Breaching this policy may result in disciplinary action for misconduct, including dismissal or contract termination. Obtaining (including accessing) or disclosing personal data in breach of the College's data protection policies may also be a criminal offence.

6 Data Protection Principles

The College complies with the data protection principles set out below. When processing personal data, it ensures that:

6.1 Data should be:

6.1.1 It is processed fairly, lawfully and in a transparent manner - make sure data subjects understand why you are collecting the data and how you will use it for specified and lawful purposes.

6.1.2 It is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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.

6.1.3 It is accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

6.1.4 It is kept no longer than necessary.

6.1.5 It is kept secure with appropriate technical and organisational measures taken to protect the information.

These principles should be considered when deciding what information to collect, when establishing procedures for processing this information and when dealing with requests from data subjects. The College is responsible for complying with the data protection principles and will demonstrate this in accordance with Article 5(2) "Accountability" by implementing policies

and procedures, technical and organisational measures and keeping documentation such as breach records and DSAR records.

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. Data subjects can also seek compensation if they suffer damage (usually physical or financial) or distress as a result of a breach of the GDPR by the business.

7 Data Subject Rights

The College has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know to whom to send it. Refer to the Data Subject Rights Request Procedure.

8 Processing Special Category Data

This includes the following personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health data; data about sex life or sexual orientation; criminal convictions or offences.

The College will apply additional organisational and technical measures to protect special category data where processed based on risk to the data subject, and it will only process special category data where it has an Article 6 lawful basis and an Article 9 exception to do so.

9 Consent

9.1 The College understands the conditions of consent as defined in Article 7 of the GDPR and will ensure that:

9.1.1 Consent is a specific, informed and unambiguous indication of the data subjects wishes.

9.1.2 The data subject can withdraw consent at any time.

9.1.3 Withdrawal of consent is as easy as it was to give.

9.1.4 Where information society services are provided to children, consent of the parent/guardian will be obtained based on the age limits defined in the country concerned.

9.1.5 Records of consent are kept as evidence.

9.1.6 The data subject is competent to give consent and is doing so freely without duress.

9.1.7 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.

9.1.8 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.

9.1.9 If any member of the College is in any doubt about these matters, they should consult DPO.

10 Security and Data Breaches

10.1 The College will always assess the risk of processing personal data to the data subject and will ensure that:

10.1.1 Personal data is stored securely using software that is kept-up-to-date and supported.

10.1.2 Access to personal data shall be role based, limited to personnel who need access and appropriate security shall be in place to avoid unauthorised sharing of information.

10.1.3 When personal data is deleted, this shall be done safely such that the data is irrecoverable.

10.1.4 Appropriate back-up and disaster recovery solutions shall be in place.

10.1.5 Staff are given information security training and information security policies and procedures are adhered to

10.1.6 Personal data is encrypted where possible at rest and in transit

10.1.7 Where possible personal data is anonymised or pseudonymised

10.1.8 All passwords used meet password policy requirements

10.1.9 Anti-malware software is deployed on all devices handling personal data

10.1.10 Paper documents containing personal data shall be stored in lockable cabinets

10.1.11 The College is also dedicated to complying with the requirements for responding to and reporting a data breach. Data breaches can come in many forms, including but not limited to:

10.1.11.1 Insider threat

10.1.11.2 Malware attacks

10.1.11.3 Accidental web exposure

10.1.11.4 Data in transit

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

All individuals covered by the scope of this policy are responsible for reporting actual, suspected, threatened or potential data breaches and for assisting with investigations as required, particularly if urgent action must be taken to prevent any or further damage.

10.2 In case there is a breach occurs/is suspected the below steps should be followed:

10.2.1 When a personal data breach is suspected, it is the responsibility of the employee who identifies the breach to report this to the Chief Operating Officer immediately to ensure the breach can be dealt with within the timescales required.

10.2.2 In the event of a data breach, employees must not speak to third parties or the press without permission from the Chief Operating Officer. Any questions from third parties related to any suspected or actual data breach should be passed to the Head of Access Participation & Marketing.

10.2.3 The Chief Operating Officer must establish whether the data breach concerns personal data where the College is acting as a data processor. If so, any data breach identified must be reported, without undue delay to the controller(s) of the personal data. Information relating to relevant controllers of personal data will be found on the Records of Processing Activities (Processor) document. Information to provide to the controller should include:

10.2.3.1 The date and time the breach was identified

10.2.3.2 A description of the nature of the breach

10.2.3.3 Categories of personal data affected

10.2.3.4 Approximate number of data subjects affected

10.2.3.5 Name and contact details of the DPO

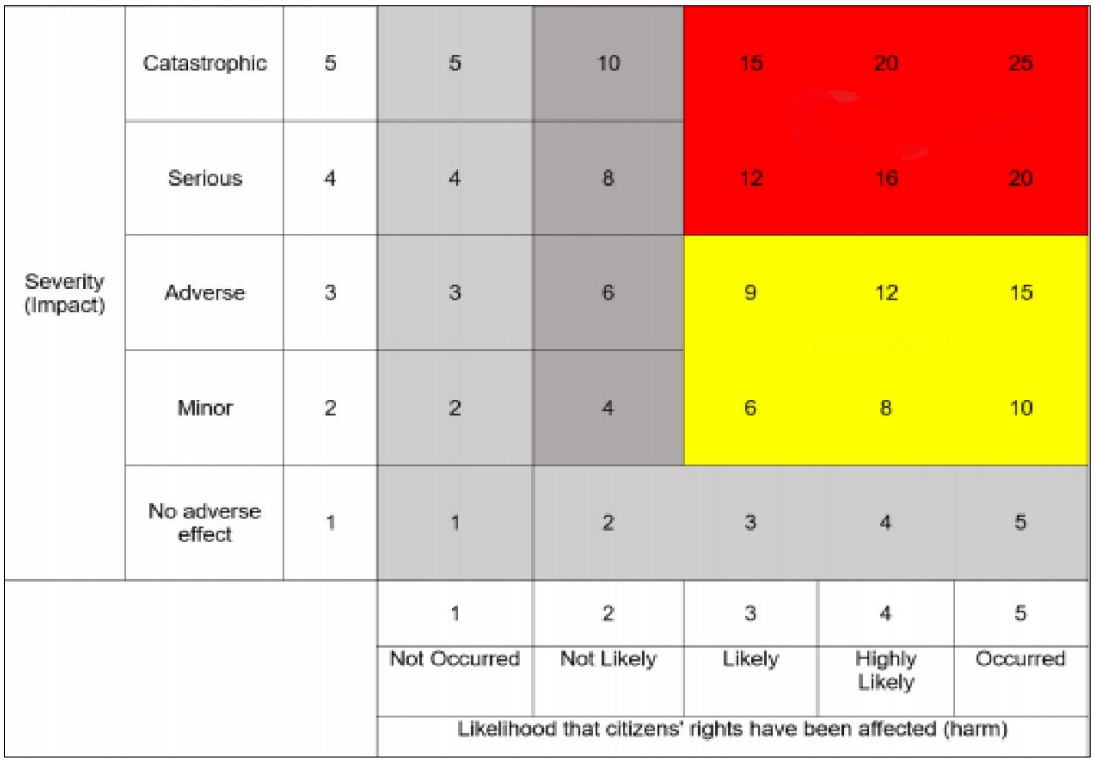
10.2.3.6 Consequences of the personal data breach

10.2.3.7 Measures taken to address the personal data breach

10.2.3.8 Any mitigating measures the controller needs to take

The Chief Operating Officer must communicate the breach to the DPO and establish whether the personal data breach should be reported to the ICO. If there If there is doubt as to whether a data breach should be reported to the ICO and/or data subject, the DPO should seek guidance from the ICO:

In order to establish the risk to the rights and freedoms of the data subject affected, the Chief Operating Officer must assess the risks in accordance with the guidelines outline below and where required, using the ICO tool here. Anything other than “grey breaches” , as below, is reportable to the ICO. Incidents where the grading results are in the red are advised to notify data subjects.



Likelihood grade	Likelihood of adverse effect	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred.	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Severity Grade	Severity of the adverse effect on Individuals	Description

1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach.
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred.	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be sending an email containing personal data about an employee to the wrong recipient.
3	Potentially some adverse effect.	An adverse effect may be release of confidential information into the public domain leading to embarrassment.
4	Potentially Pain and suffering/ financial loss.	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. A person is at risk of harassment or violence from exposed information.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence. Specific risk information for tailored response is wrong or not available.

The ICO must be notified (https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/) without undue delay but no later than in 72 hours, if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach. Any possible reasons for delay beyond 72 hours must be communicated to the ICO.

If there is a high risk to the rights and freedoms of the individuals, the College must notify without undue delay, the affected data subjects. The notification to the data subjects must be written in clear and plain language and include:

The name and contact details of any data protection officer you have, or other contact point where more information can be obtained.

a description of the likely consequences of the personal data breach; and

a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

10.3 If possible, the College should give specific and clear advice to individuals on the steps they can take to protect themselves, and what the College is able to do to help them. Depending on the circumstances, this may include such things as:

10.3.1 forcing a password reset.

10.3.2 advising individuals to use strong, unique passwords; and

10.3.3 telling them to look out for phishing emails or fraudulent activity on their accounts.

If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject, the College must take the necessary measures to ensure that the affected data subjects are notified by using appropriate, publicly available channels.

The College is also responsible for checking with sectoral regulations of the relevant parties that should be notified following a severe data breach. Significant cyber incidents may also need to be reported to the National Cyber Security Centre. Data breaches that may lead to individuals being victims of fraud should be reported to Action Fraud the UK's national fraud and cybercrime reporting centre. It may also be necessary to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

11 Data Protection by Design

Data Protection by Design allows for Data Protection to be built into a business's ethos but ensuring processes, services and other ideas are risk assessed from a GDPR point of view. The College is committed to practicing this throughout the business to ensure systems are built with data protection as the first thought, rather than an afterthought. All staff must declare new processes involving data to ensure this assessment is completed where needed. The assessment can be found in **Annex – 1.** The assessment should be submitted to the Chief Operating Officer for review.

11.1 The Chief Operating Officer and DPO will assess whether a DPIA will be necessary for the project based on whether the processing involves:

11.1.1 Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significant affect the natural person.

11.1.2 Processing on a large scale of special categories of data referred to in Article 9(1) or of personal data relating to criminal convictions and offences referred to in Article 10; or

11.1.3 A systematic monitoring of a publicly accessible area on a large scale.

If there is uncertainty as to whether it is appropriate to carry out a DPIA, the Chief Operating Officer and DPO should consult with the ICO or external consultants/legal representatives for

clarification and further guidance. If the result of any guidance is inconclusive, the default approach will be to conduct the DPIA.

11.2 If it is decided that a DPIA should be conducted using the template in Annex – 2 and steps below:

11.2.1 The project leader is responsible for conducting the DPIA with the Chief Operating Officer and DPO and for instigating the procedure.

11.2.2 The Chief Operating Officer and DPO is responsible for conducting the DPIA in partnership with the owner of any new project/system/process that is being considered.

11.2.3 The Chief Operating Officer and DPO is responsible for communication with the ICO where required (Prior Consultation as per Article 38)

11.2.4 The Chief Operating Officer and DPO is responsible for making recommendations on whether the processing can proceed.

11.2.5 The Head of QualPliance is responsible for the final decision on whether processing will proceed. Where the Head of QualPliance overrules the recommendations of the Head of Operations/DPO, this will be documented in the DPIA

11.2.6 The Chief Operating Officer and DPO is responsible for reviewing the DPIA and defining the time scale for review.

11.2.7 If the lawful basis being relied on throughout the process is legitimate interest, the above procedure should also be followed for filling out the template legitimate interest assessment (LIA) in Annex – 3.

12 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.

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

12.1.1 The individual has given their consent (e.g., a student/member of staff has consented to the College corresponding with a named third party);

12.1.2 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);

12.1.3 Where the institution is legally obliged to disclose the data (e.g., HESA and HESES returns, SLC, HEFCE, ethnic minority and disability monitoring);

12.1.4 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).

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

12.1.6 To safeguard national security*;

12.1.7 Prevention or detection of crime including the apprehension or prosecution of offenders*;

12.1.8 Assessment or collection of tax duty*;

12.1.9 Discharge of regulatory functions (includes health, safety and welfare of persons at work)*;

12.1.10 To prevent serious harm to a third party;

12.1.11 To protect the vital interests of the individual, this refers to life and death situations.

12.1.12 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.

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

12.2.1 Pass a message to the data subject asking them to contact the enquirer;

12.2.2 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.

If in doubt, staff should seek advice from Head of QualPliance and Legal Affair or Chief Operating Officer

13 Use of CCTV

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

13.1 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:

13.1.1 Any monitoring will be carried out only by a limited number of specified staff;

13.1.2 The recordings will be accessed only by the IT manager, HR manager or a director;

13.1.3 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 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.

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 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. 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.

16 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.

17 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.

18 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.

19 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.

20 Requests for Personal References

20.1 If you receive a request for a personal reference relating to a student, you should ensure that:

20.1.1 The information contained in the reference is FACTUALLY correct

20.1.2 Where possible, keep the disclosure to a minimum (student's dates of study, marks and/or degree class, registration status)

20.1.3 Sensitive data (e.g. Details of health to explain absences from the College) must not be disclosed without the explicit consent of the student

20.1.4 Where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds

20.1.5 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

20.1.6 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.

21 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, Data Protection Act 2018 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.

22 Legal Proceedings

Data Protection Act 2018 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.

23 ANNEX – 1: Data Protection By Design Checklist

#	Requirement	Example/explanation	Response	Comments
1	Has a lawful basis for processing been identified?	Legal basis includes: Performance of a contract Legal obligation Legitimate Interest Consent Vital Interest performance of a task carried out in the public interest	(Y/N)	Please identify the chosen lawful basis in here. If no lawful basis has been identified, contact your data privacy representative
2	Has all the personal data that is required to carry out this activity/process been identified and checked to make sure no additional personal data is being collected that is not needed?	You should only collect the minimum amount of personal data needed to perform the activity.	(Y/N)	Please list the personal data being collected
3	Have retention periods been identified for this personal data and recorded in the retention policy?	Identify any legal, contractual or regulatory obligations to keep personal data and consider, if none of these apply, what is a reasonable	(Y/N)	Please provide retention periods and any associated legal, regulatory or contractual requirements and ensure the document owner of the

		timescale to keep this personal data?		retention policy has been notified
4	Has a method of removing personal data for this activity/process been identified once the retention period is exceeded?	Identify ways that the data can be removed, preferably automatically. This may involve manual processes as well. Clear records and reminders need to be kept to ensure the data is removed	(Y/N)	Please give details of this method
5	Has a method for keeping the personal data for this activity/process up to date and accurate been identified?	This could involve giving the data subjects access to their data via a portal, conducting regular data cleansing activities, reminding data subjects to inform you of changes	(Y/N)	Please give details of this method
6	Have data flow maps been updated to accommodate the new process/activity	Data flow maps show, by department or function how personal data moves around your organisation and are helpful when dealing with data subject rights requests	(Y/N)	If yes, please provide details of the location of the data map

7	If consent is the lawful basis, have the requirements for consent been met?	If using consent, you must ensure: a) The data subject is giving consent by a clear affirmative action (e.g. ticking a box, signing a document) b) Consent is documented c) The data subject has been provided with clear and transparent information about the resulting processing of their data (via a privacy notice) d) Consent is freely given	(Y/N/N/A)	If Yes, please give details here of how these requirements are being met.
8	If legitimate interest is the lawful basis, has a legitimate interests assessment been carried out?	If you have not conducted an LIA, please use the provided LIA template	(Y/N/N/A)	If yes, please provide details of the LIA and whether it has been signed off by senior management or the DPO (where you have a DPO)
9	If processors are being used has a due diligence check been carried out on the processor?	Processors/service providers who process personal data on behalf of and at the instruction of your organisation should undergo a	(Y/N/N/A)	If yes, please provide details of the processors and results of the due diligence checks and location of documentation

		supplier due diligence check to verify they have suitable security and data privacy protections in place. Use the supplier due diligence checklist and document this		(including all supporting documentation such as security certification)
10	If processors are being used has a contract that meets the requirements of Article 28 been put in place with them	There should be a contract with data processing agreement that clearly outlines the data privacy obligations of the processor in accordance with the requirements of Article 28 of the GDPR	(Y/N/N/A)	If yes, please provide details of the processors and location of the contracts and whether these contracts have been checked by the DPO or legal team
11	If the personal data is transferred to third parties, has the lawful basis for doing so been identified?	See question 1	(Y/N/N/A)	If yes, please indicate which lawful basis has been chosen
12	Is the personal data being processed or transferred to a third country or organisation in a third country?	Third countries are those countries that are not part of the EEA and do not have an adequacy decision. You can see which countries have an adequacy decision here. If you are transferring personal data to one of these, there will need to be	(Y/N/N/A)	If yes, please provide details of the countries the data is being transferred to.

		additional safeguards in place such as standard contract clauses		
13	If there is special category data being processed as part of this activity, has an article 9 exception been identified for this processing?	Special category personal data includes: Religion, political opinions, ethnic origin, race, trade union membership, philosophical beliefs, genetic data, biometric data, health data, information about the data subject's sex life or sexual orientation. Article 9 exceptions can be identified here	(Y/N/N/A)	If yes, please provide details of the exception identified.
14	Has a Data Protection Impact Assessment (DPIA) been conducted?	DPIAs are needed where the processing or activity is likely to result in a high risk to the rights and freedoms of data subjects. Refer to the DPIA checklist and DPIA template	(Y/N/N/A)	If yes, please provide details of the DPIA (location)

15	Has the relevant privacy notice been updated to include the processing of personal data identified by this activity?	Your DPO or GDPR representative will help with this	(Y/N)	
16	If the source of the personal data is not directly from the data subject, have you identified the source and ensured this has been documented in an Article 14 privacy notice and issued to the data subjects in accordance with Article 14	Your DPO or GDPR representative will help with this	(Y/N/N/A)	
17	If personal data is being stored electronically, can it be exported in a commonly used machine-readable format to comply with the right to data portability?	It should be possible to export data held in a system into a csv, excel, text or other commonly used format to be sent to another controller if the data subject exercises their right to data portability.	(Y/N/N/A)	If yes, please give details
18	If automated decisions (i.e., decisions not made by humans) are made that could have legal implications or similar serious disadvantages for data subjects during the processing, is it	Contract and Consent are the two lawful bases that enable data subjects to exercise their right to portability	(Y/N/N/A)	Please indicate the necessity of processing and details of contract or consent if relevant.

	ensured that the processing is necessary for the performance of a contract or that consent has been obtained?			
19	If automated decisions (i.e. decisions not made by humans) are made that could have legal implications or similar serious disadvantages for data subjects during the processing, is it ensured that the data subject has the right to challenge the decision?	e.g. has the data subject been informed of the automated decision making via the privacy notice and how this will be handled internally?	(Y/N/N/A)	If yes, please give details
20	Can the personal data being used be anonymised or pseudonymised?	Anonymisation means the data can never be used to identify an individual, and if so, the data is no longer personal data and GDPR will not apply. Pseudonymisation does allow the possibility that the data can be used to identify an individual if additional information is provided so GDPR will still apply	(Y/N)	Please provide details.

21	Are there access controls in place to ensure access to the personal data is limited to those that need it?	Access control should be in place to restrict access. This should be configured to ensure people only see the data they need to do their job and no more	(Y/N)	Please provide details
22	Is personal data regularly backed up and data recovery tested?	This is to ensure data can be recovered (loss of access is a data breach) in the event of outage or attacks such as ransomware	(Y/N)	Please provide details
23	Is personal data encrypted at rest and in transit?	Personal data should ideally be encrypted to ensure that in the event of loss, it cannot be accessed. You should encrypt such data in line with your encryption policy	(Y/N)	Please provide details
24	If the new process involves the development of software in-house (or under your control by a third party) has the software been security tested?	Software should be security tested to identify vulnerabilities so they can be addressed before data is processed	(Y/N)	If yes, please provide details of testing and remediation efforts
25	Has the records of processing document been updated to reflect this new activity/process?	The DPO or person responsible for data privacy should update the record of processing with the information you provide	(Y/N)	

26	Have staff had suitable training to understand how the new activity/process works?	Staff should be trained to avoid accidental data breaches through lack of knowledge	(Y/N)	Please provide details of the training

24 Annex – 2: Data Protection Impact Assessment Template

o Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer to or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Process description: **The need for a DPIA was identified because:**

o Step 2: Describe the Processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
How will you collect, use, store and delete data? **What is the source of the data?** **Will you be sharing data with anyone?** **What types of processing identified as likely high risk are involved?**

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way (Is it something new)? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
What do you want to achieve? **What is the intended effect on individuals?** **What are the benefits of the processing – for you, and more broadly?**

o Step 3: Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. **Who else do you need to involve within your organisation?** **Do you need to ask your processors to assist?** **Do you plan to consult information security experts, or any other experts?**

○ Step 4: Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
What is your lawful basis for processing? **Does the processing achieve your purpose?** **Is there another way to achieve the same outcome?** **How will you prevent function creep?** **How will you ensure data quality and data minimisation?** **What information will you give individuals?** **How will you help to support their rights?** **What measures do you take to ensure processors comply?** **How do you safeguard any international transfers?**

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Very Low	LOW	LOW	MEDIUM	MEDIUM	HIGH
Low	LOW	LOW	MEDIUM	HIGH	HIGH
Medium	LOW	MEDIUM	MEDIUM	HIGH	SEVERE
High	MEDIUM	MEDIUM	HIGH	SEVERE	SEVERE
Very High	MEDIUM	MEDIUM	HIGH	SEVERE	SEVERE

- Step 5: Identify and Assess Risk

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Very Low, Low, Medium, High, Very High	Insignificant, Minor, Moderate, Major, Severe	Low, Medium, High, Severe

o Step 6: Identify Measure to Reduce Risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Tolerate, Treat, Terminate, Transfer	Low, Medium, High, Severe	Yes/no

o Step 7: Sign Off and Record Outcome

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

25 Annex – 3: Legitimate Interest Assessment Template

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside the ICO's legitimate interests guidance here.

o Part ONE: PURPOSE TEST

You need to assess whether there is a legitimate interest behind the processing.

• Why do you want to process the data? • What benefit do you expect to get from the processing? • Do any third parties benefit from the processing? • Are there any wider public benefits to the processing? • How important are the benefits that you have identified? • What would the impact be if you could not go ahead with the processing? • Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements, or e-privacy legislation)? • Are you complying with other relevant laws? • Are you complying with industry guidelines or codes of practice? • Are there any other ethical issues with the processing?
• Why do you want to process the data? • What benefit do you expect to get from the processing? • Do any third parties benefit from the processing? • Are there any wider public benefits to the processing? • How important are the benefits that you have identified? • What would the impact be if you could not go ahead with the processing? • Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements, or e-privacy legislation)? • Are there any other ethical issues with the processing?

o Part Two: NECESSITY TEST

You need to assess whether the processing is necessary for the purpose you have identified.

• Will this processing help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?
• **Will this processing help you achieve your purpose?** • **Is the processing proportionate to that purpose?** • **Can you achieve the same purpose without the processing?** • **Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?**

o Part 3: balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests. First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?
• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?

○ PART FOUR: REASONABLE EXPECTATIONS

- Do you have an existing relationship with the individual?
- What is the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation?
- Are there any other factors in the circumstances that mean they would or would not expect the processing?

- Do you have an existing relationship with the individual?
- What is the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation?
- Are there any other factors in the circumstances that mean they would or would not expect the processing?

○ Part five: LIKELY IMPACT

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?

• Would you be happy to explain the processing to individuals? • Can you adopt any safeguards to minimise the impact? • Can you offer individuals an opt-out? YES/NO
• What are the possible impacts of the processing on people? • Will individuals lose any control over the use of their personal data? • What is the likelihood and severity of any potential impact? • Are some people likely to object to the processing or find it intrusive? • Would you be happy to explain the processing to individuals? • Can you adopt any safeguards to minimise the impact? • Can you offer individuals an opt-out? YES/NO

○ Part six: making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether you can apply the legitimate interest's basis.

Can you rely on Legitimate Interests for this processing?	
Completed by	
Date	