COLÁISTE CHEATHARLACH
NAOMH PÁDRAIG
CARLOW COLLEGE
ST. PATRICK'S

Data Protection Policy: Appendices

TABLE OF CONTENTS

	Page
Appendix 1: Data Use and Security Guidelines	1
Appendix 2: Records of Processing Activities	6
Appendix 3: Data Protection and IT Supplier Assessment Form	34
Appendix 4: Template Data Processing Agreement	41
Appendix 5: Collaborations with External Partnerships – Data Protection Assessment Form	51
Appendix 6: Data Subject Request Form	57
Appendix 7: Template Data Protection Impact Assessment	61
Appendix 8: Personal Data Breach Response Plan	67
Appendix 9: Online Meetings and Events	70
Appendix 10: Privacy Notice	73
Appendix 11: Template for Legitimate Interests Assessment	74
Appendix 12: Guidelines on Surveys	78
Appendix 12.1: Survey Approval Form	84
Appendix 12.2: Documentation to be sent to the DPO	85
Appendix 13: Information / Documentation Flows to the DPO	87

Appendix 1: Data Use and Security Guidelines

COLÁISTE CHEATHARLACH
NAOMH PÁDRAIG
CARLOW COLLEGE
ST. PATRICK'S

Data Use and Security Guidelines

Users of Carlow College personal data, including employees and learners, must comply with these guidelines. This is not intended to be an exhaustive list of safeguards. Further measures may be in place regarding technical security in the policies of IT Services. While the Data Protection Policy refers to personal data, these guidelines are also valuable to protect non-personal College records.

Collecting and creating records

- Double check your recipient when sending emails.
- Password-protect email attachments containing personal data and confidential business information. Do not email the password. Communicate it by a different means e.g. text message or phone call.
- Do not collect personal data unless it is required e.g. make surveys anonymous.
- Official records should be kept in the College's electronic or manual systems.
- Use College devices, where possible.
- If it is necessary to use a personal device, particularly a shared device, ensure that College records are kept securely and confidentially.
- Do not use personal accounts to create or store official records.
- If personal accounts/devices must unavoidably be used, copy records to College systems/devices as soon as possible and delete them from personal accounts/devices.
- Keep personal data up to date and make requested changes promptly e.g. change contact details on request.
- While straightforward updates may be made e.g. change of address on a system, do not alter a document created by another employee without their permission.
- Personal data is not to be posted on public noticeboards or other public spaces.
- When recording personal data, check back with data subjects that what you have recorded is accurate, when appropriate e.g. send them a copy or read it back.
- Ensure that your communications are written in an objective, truthful, responsible and accurate manner.
- Pseudonymise or anonymise personal data, as appropriate, when it is no longer required to identify individuals.
- Carry out a Data Protection Impact Assessment (DPIA), where required.
- Consider data protection issues early in a new project and contact the DPO.
- Carry out audits on data quality e.g. check for errors.

- Design forms to collect the minimum personal data necessary to fulfil your purpose.
- Collect personal data in a privacy friendly manner e.g. sign-in books used by multiple persons to record their contact details might be replaced with individual use forms in paper or electronic formats.

Access

- Access permissions for both manual and IT systems should align with employee duties.
- Do not access records that you have not been authorised to view i.e. records unrelated to your duties or for which you have not been granted access permissions.
- Employees may have access to personal data in systems that they do not require e.g. about learners that they do not teach. Employees should only access personal they require to carry out their duties.
- Keep your password secure and private to you.
- Use robust passwords. They should contain a mixture of letters and other characters (see advice on pp5-6 here).
- Change your passwords regularly.
- Do not use the same password for multiple accounts.

Respecting other people's privacy

- Photographs may be personal data. Ensure that you only use photographs in a manner allowed by Data Protection law. This may vary on the circumstances, but photographs require either consent or a legitimate interest (e.g. people would likely not be surprised to be photographed at a conferring ceremony). However, care should still be taken when deciding how to use photographs, and consideration given to what people might expect photographs would be used.
- If holding an event, inform attendees if photographs will be taken or the event recorded. This can be done by posting notices in the area, informing people when inviting them or during the booking process etc. Such notices can suggest that people speak to the photographer if they do not wish to be photographed. Notices should also indicate if it is intended to make photographs available e.g. on social media. The DPO can assist event organisers to draw up such notices. If an individual objects to the publication or other use of their photograph, comply with their wishes.
- Consider the data protection and privacy rights of others before you share an image or video of a video call that includes the image, voice or contact details of participants. Such sharing is discouraged.
- Covert recording of employees, learners or any other person with whom employees or learners come into contact in the workplace or through the course of duties of studies is not permitted.

Disclosing personal data

- Double check your recipient when sending an email.
- Password-protect email attachments containing personal data and confidential business information. Do not email the password. Communicate it by a different means e.g. text message or phone call.

- Send group emails via 'bcc' where it is not appropriate that recipients see each other's email address e.g. external email addresses; marketing mailing lists; where membership of a group should not be disclosed to others e.g. Counselling clients.
- In general, employees are only to disclose learner personal to parents/guardians or other family members with the learner's written consent. This applies to all data including about fees, attendance, grades etc. There are extremely limited exceptions to this i.e. in a life-and-death situation.
- References about learners should only be provided to prospective employers, other educational institutions etc with the learner's consent.
- Student ID numbers are personal data as they are linkable to an individual. They cannot be used to anonymise information about learners.
- Share personal data and other records with colleagues on a need to know basis only.
- If authorised employees from other departments need to borrow files from your office, implement a sign in/out book. Agree a borrowing period and issue a reminder if not returned on time.
- Do not share personal data or other confidential information acquired through your official duties on social media.

Disposing of records

- Dispose of personal data and other confidential records securely. Shred paper records.
- Paper records are not to be disposed of in wastepaper or recycling bins.
- Return devices to IT Services for secure deletion of data and disposal.
- Dispose of records in accordance with the Records Retention Schedules.
- Some records are designated 'archival', which means that they are kept on an ongoing basis. Transfer them to the Delany Archive.

Keeping records secure

- All personal data and non-personal business records are confidential. Employees are to maintain and protect this confidentiality.
- Notify the DPO immediately of any incident where data has been put at risk or you suspect a potential or actual personal data breach or incident.
- Take appropriate methods to secure records when leaving your workspace e.g. lock your screen; lock the door; store paper records securely.
- Do not leave the key in your office door.
- Do not leave unauthorised people alone with personal data or other confidential business records.
- Keep records out of arm's reach to visitors.
- Do not allow your computer screen to be viewable from a public area or to an unauthorised person.
- Locked storage units are ideal for paper records.
- Do not remove records from the College premises unless necessary.

- Return borrowed records to the College as soon as you are finished with them.
- Do not leave records on view in your car or in your car overnight.
- Assignments and examination scripts are not to be corrected in a public place.
- Do not store records on removable devices, such as memory sticks, unless necessary
- Do not print unnecessary paper copies of documents.
- Do not leave personal data or other confidential records unattended at photocopiers or other public locations.
- Employees who are changing position or leaving the College's employment are to ensure that they leave all relevant records for their successor.

New colleagues and volunteers

- Appoint a 'buddy' to new employees to explain procedures for handling personal data and other records.
- Volunteers and people on work experience should have limited or no access to personal data and other confidential records.

Working remotely

- It is important to understand that the Data Protection Policy applies in all locations where Carlow College personal data is processed, including remote working locations.
- If particular arrangements have been put in place for you, ensure that you abide by them.
- Ensure that you are particularly careful about the security and confidentiality of personal data (and non-personal records) if using a shared device. Work records should be stored in College systems, wherever possible. If it is necessary to store data locally on a device, ensure that documents / folders are protected by strong passwords.
- The Data Protection Commission (DPC) has provided guidance which is also applicable.[1] Most of the guidance is already covered by this Policy, however, the following may additionally be relevant:

<u>Electronic records</u>

  - Ensure that any device you use has the necessary updates, such as operating system updates (like iOS or Android) and software/antivirus updates.
  - Ensure that your devices are turned off, locked or stored carefully when not in use
  - Use effective access controls (such as multi-factor authentication and strong passwords). and, where available, encryption to restrict access to the device, and to reduce the risk if a device is lost or stolen.
  - When a device is lost or stolen, take steps immediately to ensure a remote memory wipe, where possible.

[1] https://www.dataprotection.ie/en/dpc-guidance/blogs/protecting-personal-data-when-working-remotely [accessed 29 September 2021].

- Where possible, only use the College's trusted networks or cloud services, and comply with any organisational rules and procedures about cloud or network access, login, and data sharing.
- If you are working without cloud or network access, ensure any data stored locally is effectively backed up in a secure manner.

Paper records

- Ensure the security and confidentiality of paper records, taking particular care of special categories of personal data.
- Only remove paper records from the College premises when it is strictly necessary, and return them to the College as soon as possible.
- Ensure that paper records are disposed of securely.
- Keep a written record of which records and files have been removed from the College premises, in order to maintain good data access and governance practices. Functions where paper records are shared may find it useful to create a function-level register.

Appendix 2: Records Processing Activities

COLÁISTE CHEATHARLACH NAOMH PÁDRAIG
CARLOW COLLEGE ST. PATRICK'S

Records Processing Activities (Draft to 30.11.2021)

Controller: Carlow College, St Patrick's, College Street, Carlow

Data Protection Officer: Bernie Deasy, dataprotection@carlowcollege.ie; 059-9153200

Contents

Records Retention Schedules 7
Technical & Organisational Security Measures 7
Data Recipients 7
Table 1: Carlow College, St Patrick's as a Controller....8
Library & Archive....16
Information & Communications Technology....17
Students' Union 18
Building Services 27
Accommodation....32
Section 2: Carlow College, St Patrick's as a Processor....33

Records Retention Schedules

Retention timeframes are detailed in Records Retention Schedules, which are available in the Records Management Policy.

Technical & Organisational Security Measures

In general, electronic records are held in password-controlled systems, and paper records are held securely in locked offices or units. All personal data is disposed of securely. A fuller description of technical and organisational security measures is available in the Data Protection Policy.

Data Recipients

External data recipients are indicated in the following tables. Some data recipients may have general applicability e.g.

- As many records are created and/or held electronically in systems, the providers of such systems, including but not limited to Microsoft, BrightHR and Ellucian (SRMS provider).
- Service providers, including but not limited to legal advisors, insurers and auditors in order that the College can avail of their services.
- An Garda Síochána, Tusla and other statutory and law enforcement agencies, in order that the College complies with relevant laws, regulations and the rules of various schemes.
- To permit compliance with a court order.
- Validating and regulatory bodies, including but not limited to Quality and Qualifications Ireland (QQI) and CORU.

Carlow College will ensure that data sharing complies with data protection law.

Table 1: Carlow College, St Patrick's as a Controller

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
1	Prospective learners (pre-application)	To answer queries	Contact details, details of queries	Legitimate interest		Admissions Office, Student Recruitment Office			
2	Prospective learners (pre-application)	To administer mailing lists	Contact details, consent	Consent		Student Recruitment Office			
3	Prospective learners (pre-application)	To answer queries about disability and learning difference supports	Contact details, details of queries	Legal obligation	Public interest	Student Services			
4	Applicant learners Referees of applicant learners	To administer applications	Information supplied to the CAO, CCSP or any third party when applying. May include: contact details, DOB, CAO No., nationality, educational history, employment history, proof of qualifications, references, personal essay, English language standard, mature student status, disability/learning difference, programme choice, interview records, decisions on and correspondence about applications. Study Abroad applicants also supply: emergency contact details, passport photo page, module selection.	Contract, legal obligation	Public interest	Admissions Office, interview panel, Programme Director, International Office	CAO, referees, Study Abroad and Exchange Programme providers, other collaborative providers	CAO	Study Abroad and Exchange Programme providers, USA: Standard Contractual Clauses
5	Applicant part-time learners	To assess if fee reduction can be given	Evidence of DEASP payment	Contract		Admissions Office			
6	Learners	To provide education services to you; to verify your attendance and results/awards.	Dates of attendance, name of programme, results, awards made, name, gender, photograph.	Contract		Teaching and administration staff	Programme validator, SRMS provider (Ellucian)		
7	Registered learners	To assess fee status	Proof of residency, proof of identity, declaration re previous third level education	Contract, Public interest	Public interest	Admissions Office	Department of Education (free fees)		

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
8	Learners	To comply with study visa requirements, including monitoring attendance	Study Visa, attendance records	Contract, legal obligation		International Office	Irish Naturalisation and Immigration Service		
9	Learners Parents/guardians of learners under the age of 18	To conduct Garda or police vetting	Contact details, DOB, current and past addresses, proof of identity, convictions, vetting disclosure from An Garda Síochána, police clearance from other jurisdictions	Legal obligation		Liaison Person, Placement Coordinator	National Vetting Bureau. The fact that a learner has been satisfactorily vetted may be communicated to a practice placement if a Section 12(3A) agreement exists.		
10	Learners	To assess vetting disclosures where convictions or specified information is returned	Disclosure details, meeting and decision records.	Legal obligation		Liaison Person, Placement Coordinator, Programme Director, Practice Placement Advisory Committee, appeal panel.			
11	Learners, emergency contact, emergency services	To respond to emergency situations involving learners; to notify the learner's emergency contact	Contact details, nature of relationship with learner, details of emergency event	Legitimate interest (to notify learner's emergency contact)	Vital interests	As required e.g. Programme Director, Nurse	Emergency contact, emergency services		
12	Learners	To monitor attendance. Learners may supply medical certification to excuse absence.	Names, attendance records, records of addressing poor attendance and correspondence with learner about same.	Contract, public interest, legitimate interest (to monitor learner engagement)		Teaching staff, LIRO, Academic Advisors, International Officer, Nurse, Academic Administration, Placement Coordinator, Practice Placement Advisory Committee	Irish Naturalisation and Immigration Service; Study Abroad providers		Study Abroad providers, USA: Standard Contractual Clauses

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
13	Learners, staff	Class recordings	Names, images, contributions to classes, discussion posts	Legitimate interests (to make class recordings available to learners who are unable to attend in person or for asynchronous access)		Defined by Moodle access permissions	Learners, Microsoft		
14	Learners	To administer scholarships and prizes	Names, applications, photographs of awardees	Legitimate interest (to reward learner achievements)		Student Recruitment Office, Registrar's Office	May be published on the world wide web, media outlets or in conferring booklet, sponsors of prizes		
15	Learners	To make returns of registered learners to the DEASP	Name, address, DOB, programme, duration of programme, attendance requirements, grants or payments made to learner by any body, authority, institution or fund	Legal obligation		Admissions Office	DEASP		
16	Learners	To administer requests for assistance with academic matters e.g. extensions, extenuating circumstances, Essay Doctor, examination deferrals	Contact details, requests for assistance	Contract	Consent	Depending on which process applies, may include: College Nurse, Writing Development Tutor, Academic Administration, Exams Officer, Programme Director, Registrar's Office			
17	Learners Other involved parties e.g. complainant, respondent, witness	To make decisions and conduct investigations and appeals under policies such as disciplinary, harassment, bullying, grievances, complaints, fitness to	Details of matters under investigation, decisions, appeals.	Contract		Depends on the process. May include e.g. Registrar's Office, investigator, Placement	Study Abroad or other collaborative provider		Study Abroad providers in USA: Standard Contractual Clauses

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
		practise, fitness to continue in study.				Committee, Academic Advisor			
18	Learners	To assess applications for disability supports and reasonable accommodations; to administer disability supports and reasonable accommodations, to report to the HEA regarding the Fund for Students with Disabilities	Learner case files including contact details, needs assessment, educational psychological report, medical report, agreements regarding use of assistive technology by learner, consents to share information, records of sessions with tutors	Legal obligation, contract, public interest	Public interest, consent (to share information with College services and/or placement provider)		Study Abroad provider, HEA, placement providers, Grammarly		Study Abroad providers in USA; Grammarly: Standard Contractual Clauses
19	Learners	To administer learner withdrawals, deferrals and admissions; to inform relevant College services to close/open accounts etc., and external bodies.	Contact details, ID number, programme and stage, whether learner is a grant holder, entry route, nature of circumstances, future education plans, academic transcripts	Contract, consent (some questions are optional)		Admissions Office, LIRO, Registrar's Office, relevant College services (e.g. Reception, IT Services, Student Services)	Grant provider (e.g. SUSI), collaborative provider, Study Abroad provider, other HEIs (at request of learner)		Study Abroad providers in USA: Standard Contractual Clauses
20	Learners	To supervise research	Supervision plan	Contract		Supervisor			
21	Learners	To administer research ethics applications and appeals	Contact details, details of research	Contract	Research	Supervisor(s), Research Ethics Advisory Committee			
22	Learners	To assess academic work: assignments (including dissertations), examination scripts. To maintain academic work submitted through Turnitin for academic integrity purposes.	Details of submitted academic work, metadata e.g. online identifiers collected by Turnitin, feedback	Contract, legitimate interest (academic integrity)	Research	Academic staff, Academic Administration	External Examiner; Turnitin; dissertations are potentially publicly accessible if deposited in the College Library with learner's consent		
23	Learners	To administer examination appeals	Contact details, details of appeal, outcome	Contract		Registrar's Office, Exams Officer, Academic Administration			
24	Learners	Examination hall administration e.g. learner	Learner attendance, reports of alleged incidents of	Contract	Consent	Invigilators, scribes, Exams			

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
		attendance, provision of reasonable accommodations, reports of alleged incidents of cheating etc.	cheating (may include photographs), reasonable accommodations			Officer, Registrar's Officer, Academic Administration			
25	Learners, academic staff	Reporting by External Examiners	Commentary on learner performance and internal examination process	Public interest		Registrar's Office, Programme Director, Programme Boards, Academic Council, Academic Committee of Governing Body. Redacted where necessary	Validating body, External Examiners		
26	Learners Emergency contacts, employees of host institutions	To administer the Exchange Programme for learners of CCSP, to decide on applications and communicate with institution visited by learner	Contact details, DOB, gender, programme and stage, course selection, conduct agreement. Records which are incoming to CCSP from collaborative providers are academic transcripts, health data and disciplinary records.	Contract	Consent	International Office	Collaborative providers		Collaborative providers, USA: Standard Contractual Clauses
27	Learners Recipient of reference	To provide references about learners	Details of reference	Consent		Referee	Recipient of reference		Possibly depending on learner request and destination of reference: consent of learner.
28	Learners Employees	To assess satisfaction of learners with teaching and other services provided to them	Varies depending on the survey. Some surveys are anonymous or pseudonymous.	Legitimate interests (to assess learner satisfaction, plan for the future), public interest. Consent may be asked.	Consent may be asked.	Varies depending on the survey	Survey platform e.g. SurveyMonkey		SurveyMonkey is based in the US and is used for some surveys. Standard Contractual Clauses.
29	Learners Employees of placement	To organise, supervise and assess learner placements	Name, programme and stage, contact details, visit reports, correspondence, agreements with placement, disciplinary and attendance	Contract	Consent if there is communication with placement at learner's	Placement coordinator, supervisor	Placement		

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
			matters, assessment, reasonable accommodations		request about reasonable accommodations				
30	Learners	To create a record of attendance and participation in CCSP Committee meetings.	Names, positions, details of attendance and participation	Legitimate interest (to have learner representation on committees)		Participants and as required for business or other legitimate purposes.			
31	Learners	Information about learners' contractual terms and conditions	Terms and conditions	Contract		As defined by SRMS permissions	SRMS provider (Ellucian)		
32	Learners Attendees	To organise and administer conferring ceremonies	Names, learner attendance and award, prize nominees and awardees, academic dress requirements, photographs	Contract, legitimate interest (to create a record of an important College event)		Conferring Committee, staff who decide prize winners, Marketing Office	The conferring ceremony is regarded as a public event. Photographs may be published on CCSP's website or social media, sponsors of prizes		
33	Learners	To administer mailing lists to inform learners about CCSP events and other CCSP information, and to enable learners to participate in College life	Email address	Legitimate interests (to inform learners about CCSP events and information)		Mailing list administrator, Marketing Office	Mailing list platform		
34	Learners, alumni	Data that is retained permanently for archiving and research purposes, and to fulfil learner requests (e.g. for references and transcripts)	Contact details, DOB, Student ID No., programme, grades, awards	Legitimate interests (to fulfil learner requests for references and transcripts)	Archiving in the public interest and/or historical research	As defined by SRMS permissions	SRMS provider (Ellucian); Delany Archive Trust. CCSP is a partner in this independent charitable trust. It operates under its own suite of policies and have safeguards in place to protect the rights of data subjects.		
35	Learners Parents / guardians of	To provide counselling services to learners, including assessing suitability for counselling	Contact details, DOB, civil status, family details, medications and health issues, GP name, reason for	Contract, legal obligation, vital interests	Consent (for data sharing with external health	Counselling Service	GP, Self-Harm Intervention Programme (HSE)		

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
	learners under 18, family members		attending, counselling plan, appointments, clinical notes, if referred to other services, assessment of risk to self or other individuals by learner, parent/guardian consent for learner under 18		providers), health care				
36	Learners	Provision of health care by the College Nurse to learners; making appointments with the contracted external GP surgery and administration of this contract; excusing ill learners from class.	Contact details, General Medical Services card number, DOB, programme details, contact details of learner's GP, medical history including medication, allergies, appointment details, notes of consultations, details of vaccinations administered by contracted GP's surgery	Contract	Health care, vital interests, consent	Nurse, Counselling Service (they make may appointments with the contracted GP surgery in the Nurse's absence), Academic Administration (emails excusing learners from class)	Contracted GP surgery, learner's own GP		
37	Learners, alumni	To assist learners and recent graduates to prepare applications for jobs and future study, advertising vacancies	Contact details, curriculum vitae	Contract, legitimate interests (assisting learners / alumni to prepare applications for jobs and future study)		Careers Office			
38	Employees, learners, stakeholders such as external examiners and placement provider staff	To comply with requirements of programme validation/ review, and institutional review, by regulatory bodies and programme validators	Names and contact details of employees and stakeholders, external examiner reports, curriculum vitae of teaching staff	Public interest		Office of the Registrar, Quality Assurance Officer, staff project teams responsible for validation and reviews	Validating and regulatory bodies (e.g. QQI, Institute of Technology, Carlow, CORU)		
39	Learners, staff, external examiners	To provide a Virtual Learning Environment with plug-in for student assessment (Moodle with Turnitin plug-in)	All users: audit trail, password, IP address, email address, name, discussion forum posts, data entered voluntarily (e.g. photo).	Contract, legitimate interests (environments where		Teaching and support staff	Enovation (Moodle provider); Turnitin		

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
			Learners: assessment submissions and feedback, surveys, quizzes, class lists.	learners can communicate with each other)					

Library & Archive									
No.	**Data subjects**	**Purposes of Processing**	**Categories of personal data**	**Article 6 legal basis**	**Article 9 legal basis**	**Internal users**	**Possible external recipients**	**Joint controller**	**3rd country transfer and safeguards**
40	Learners, employees, Library staff	To register Library users and administration of borrowing records on Heritage system.	Both employees and learners: name, borrowing records, password, logins. Employees: borrower number. Learners: student ID No., contact details, programme details, barcode number, record of fines. Library staff: audit trail on Heritage.	Contract, legitimate interests (operation of Library service and collect fines)		Library; details of unpaid learner Library fines sent to Academic Administration	IS Oxford (provider of Heritage system)		
41	Donors of items to the Library	For collection management purposes	Names, contact details, details of correspondence	Legitimate interests (collections management)		Library			
42	Learners	To administer credit available to learners for photocopying and printing on Library computers	Name, student ID No., job details, amount of credit available, password	Contract		Library			
43	Learners, employees, third parties	Administration of incoming and outgoing inter-library loans	Contact details, requested item(s)	Contract		Library			
44	External visitors using Library facilities	To record details of individuals to whom Library facilities are extended	Contact details, details of visit	Legitimate interests (for security and health and safety purposes)		Library, Facilities Manager			
45	Employees	To create a record of Library stock requested by employees	Name	Legitimate interests (collection management)		Library			
46	Learners	To order and process payment for books ordered by the Library (Bookshop) on behalf of learners and staff	Contact details, item ordered and payment	Contract		Library			
47	Donors of items to the College Archive (see also the ROPA of the Delany Archive Trust)	For collection management purposes	Name, contact details, correspondences, deposit agreements	Contract		Archivist, President's Office			

Information & Communications Technology									
No.	**Data subjects**	**Purposes of processing**	**Categories of personal data**	**Article 6 legal basis**	**Article 9 legal basis**	**Internal users**	**Possible external recipients**	**Joint controller**	**3rd country transfer and safeguards**
1	Staff, learners	IT support requests	Contact details, details of queries and responses	Legitimate interests (to maintain the functioning of systems and user support)		IT Services			
2	Staff, learners	Provision of training	Name, attendance records	Legitimate interests (to provide training opportunities to staff and learners)		IT Services			
3	All users	Wi-Fi access	Device and connection information including IP address, MAC address, client hostname, bandwidth usage and download capacity, date and time of last connection, location analytics.	Legitimate interests (to make Wi-Fi available, technical security)		IT Services			
4	Employees, Governors, Trustees, learners, alumni	To communicate important College information via text message	Name, mobile phone number, group assigned to	Legitimate interests (effective communication of important information)		President's Office, Reception, Academic Administration	SMS Solutions Ireland (processor)		
5	Employees	Phone records (mobile phones)	User name, phone number, all numbers called, bills	Contract		Accounts	Mobile phone provider		
6	Users	To provide access to systems; user analytics	Passwords; details of logins	Legitimate interests (to provide access to systems and usage)		IT Services and other system administrators	System provider		
7	Users	To provide printing and scanning services	Copied and scanned documents	As indicated by legal bases listed throughout the ROPA		IT Services	Copymoore, Google (Gmail)		

Students' Union									
No.	**Data subjects**	**Purposes of processing**	**Categories of personal data**	**Article 6 legal basis**	**Article 9 legal basis**	**Internal users**	**Possible external recipients**	**Joint controller**	**3rd country transfer and safeguards**
1	Learners (candidates for election and electorate)	To oversee the election of Students' Union Officers	Names, programme and stage, results of election	Legitimate interests (employee may act as Returning Officer)		Returning Officer	Results of election announced to learners, staff; may be published on social media. The returning officer may be any person proposed by the SU Executive and ratified by the Class Rep Council.		

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
1	Learners, fee payers	To administer fees and other payments owed by learners	Names, contact details, amounts owed, payment plan, bank account information	Contract		Accounts, Admissions Office	SRMS provider, payments services provider		
2	Learners	Administration of Free Fees Initiative	Name, student ID No., fee payable less learner contribution, status (whether eligible for free fees or not), indication as to whether learner left due to unspecified medical issue	Public task	Public interest	Admissions Office	Department of Education		
3	Learners	To administer financial assistance to learners (Chaplaincy Assist Fund)	Application: contract details, current financial supports Accounts of fund: name, amount awarded	Legitimate interests (assisting learners in financial difficulty)		Chaplain			
4	Suppliers, independent contractors	To administer contracts with suppliers and independent contractors	Names, contact details, contract details, correspondence, payments, banking information, PPSN, VAT No.	Contract, consent (for trade references - contact details)		Accounts	Sage, Revenue Commissioner (third party returns), other suppliers		
5	Employees	To administer petty cash	Names, amounts received	Legitimate interests (financial administration)		Reception, Accounts			
6	Employees, independent contractors	To administer payroll to employees. Includes salary/wages, increments, payments for other purposes e.g. travel, exam corrections, training etc, deductions e.g. LPT, Bike to Work Scheme, trade union membership	Names, contact details, banking information, PPSN, claim forms, banking information, taxation information	Contract	Employment law	Accounts	Sage, Revenue Commissioners		
7	All payees and persons whom the College pay	To keep banking records e.g. lodgements, cheque journal, bank statements, bank reconciliations reports	Name, contact details, bank details, amount, date, reason for payment	Legitimate interests (financial administration), contract		Accounts	Sage, Bank of Ireland		
8	Legal representatives	Administration of bequests to CCSP	Contact details	Legitimate interests (financial administration)		Accounts, President's Office			
9	Donors, sponsors	Administration of sponsorship and donations – incoming and outgoing	Contact details, amounts, correspondence	Legitimate interests (financial administration)		Accounts, President's Office	Revenue Commissioners (Charitable Donation Scheme)		
10	Employees	To administer timesheets (payroll purposes and claims re ESF-funded tutors)	Contact details, hours worked, line manager authorisation	Contract, Public interest		Accounts, line manager	Auditing wing of the Department of Education & Skills for ESF timesheets		

	Employees, former employees	To administer staff pensions and PRSAs	Contact details, details of payments	Contract		Accounts	Pension provider			,
11	Employees	To administer employment schemes e.g. Wage Subsidy Scheme	Names, PPSN, hourly rate and hours, wage subsidy claimed, gross wages paid, employer declaration (completed through DEASP portal)	Public interest		Accounts	DEASP			
12	Employees	To process and administer applications under the Bike to Work Scheme	Application, details of items purchased through scheme	Contract, public interest		Accounts	Suppliers			
13	Employees	To provide facility whereby employees can save money	Names, amounts of money saved and paid out	Legitimate interests (to provide facility whereby employees can save money)		Accounts				
14	Employees	Administration of Social Protection documentation e.g. certifying holiday entitlement of an education sector worker, unemployment and social welfare claims	Contact details, PPSN, details of employment (e.g. hours employed, when last worked and expected to work again, holiday pay)	Contract, public interest		Accounts	Usually given to employee but may be sent to DEASP at employee's request			
15	Employees, learners, third party stakeholders	To conduct audits – financial and process-based. Includes audits conducted by internal and external auditors.	As required. Internal audit is subject to the Internal Audit Charter.	Legitimate interests (quality assurance); legal obligation (Charities Act 2009)		Accounts, any function that is audited	Auditors			
16	Persons hiring College facilities	To consider applications to hire College facilities and record use	Names, contact details	Contract		Facilities Manager				
17	Employees and contractor / supplier employees	To administer contracts and service agreements	Names, contact details, correspondence details	Contract		Relevant staff	Service providers			

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
1	Job applicants, interview board members	Recruitment	Informal enquiries, CV and covering letter, proof of qualifications, references, interview records (including details of reasonable accommodations) and subsequent communications to applicant	Contract	Employment law	HR, line manager, interview board members	Referees		
2	Senders of unsolicited CVs	To administer unsolicited CVs	CVs	Legitimate interests (staffing)		HR			
3	Employees	To enable communication	Personal and work contact details including postal address, email address and phone numbers	Contract		HR, line manager, Reception (phone numbers only), other employees, as necessary	BrightHR		
4	Employees, emergency contacts	To notify emergency situations to employee contacts and the emergency services	Contact details, details of emergency events	Legitimate interests (to notify emergency situations)	Vital interests	HR, line manager, as required	BrightHR		
5	Employees	To verify professional accreditation and insurance	Proof of professional accreditation and insurance	Contract		HR	QQI		
6	Employees	To verify work permits of non-EU citizens	Work permits	Contract, legal obligation		HR	Department of Enterprise, Trade & Employment, Irish Naturalisation and Immigration Service		
7	Successful applicants, employees	To vet prospective and current employees	Vetting applications, vetting disclosures from the National Vetting Bureau, police clearance from other jurisdictions, meetings records and related correspondence if convictions are disclosed	Legal obligation		Employee Liaison Person, HR, Garda Vetting Panel (if required)	National Vetting Bureau		

8	Employees, family members of employees where relevant	To administer all types of employee leave, including, annual, career break, sabbatical, term time, maternity and paternity parental, time in lieu, sick leave, force majeure	Applications, decisions, supporting documentation, records of leave taken	Contract, legal obligation	Employment law, working capacity of employee, preventive or occupational medicine	HR, line manager, Accounts (leave dates and type)	BrightHR		
9	Employees	To manage the employment contract (general) e.g. contract changes	Contract, contract notes, probation records, associated correspondence	Contract	Employment law	HR, line manager	Legal advisors		
	Employees, any other involved party (e.g. witness)	To manage the employment contract: case files with regard to issues such as processes or investigations under policy (e.g. mediation, grievance, dignity and respect, disciplinary matters)	Details of matter under investigation and associated correspondence	Contract	Employment law	HR, line manager, mediators, investigators	External mediator or investigator, legal advisors, Workplace Relations Commissions		
10	Employees	Referring employees to the Employee Assistance Programme (EAP)	Contact details, details of referral	Contract	Working capacity of employee, preventive or occupational medicine	HR, line manager	EAP provider		
11	Employees	To conduct performance reviews and put Personal Improvement Plans in place, where necessary	Contact details, role details, objectives setting and review	Contract		Line manager, HR			
12	Employees	Election or selection of employees to internal committees and external bodies	Names, details of position	Contract		May be notified to all staff or publicly	Relevant external body		
13	Volunteers, including work experience	To manage the volunteering / work experience relationship	Contact details, agreement, hours volunteered	Contract		HR, line manager / supervisor	Relevant external body		
14	Employees	To certify salary and other employment information at the request of employees	As dictated by questions on the form presented to the College	Legitimate interests (to fulfil employee request)		HR, Accounts			
15	Former employees	To complete statements of service for former employees at their request	As dictated by questions on the form presented to the College	Legitimate interests (to fulfil former employee request)		HR			
16	Employees, former employees	To provide references at the request of employees or former employees	Reference, dates of employment	Consent		HR, line manager or other relevant staff			

17	Employees	To conduct surveys in order gather information for various purposes	Surveys are usually anonymous, but replies may sometimes make individuals identifiable	Varies depending on the survey e.g. consent or legitimate interests (information gathering)	e.g. explicit consent	HR, other staff responsible for data analysis			SurveyMonkey is used for some surveys and exports data to the US. Standard Contractual Clauses.
18	Employees	To provide important information to employees e.g. new appointments, retirements, resignations, bereavements	Name, position, details of event	Legitimate interests (to provide important information to employees)					
19	Employees	To record training undertaken by employees and related records such as records of educational financial assistance. See also references to employee training in the ICT and Health & Safety sections.	Name, details of training and qualifications, records relating to educational financial assistance	Contract, legitimate interests (to records details of training undertaken by staff)		HR			
20	Employees	Timesheets to record hours worked by employees in accordance with the Organisation of Working Time Act, 1997	Contact details, hours worked	Legal obligation		HR, line manager			
21	Employees, successful candidates	Records arising from referring employees and successful candidates to the Occupational Health Provider (OHP) for employment purposes, disability support	Contact details, details of referral, incoming report from the OHP	Contract	Employment law	HR	OHP		
22	Employees	To ensure that employees who drive for work have a valid driver's licence and insurance	Driver's licence, insurance policy	Contract		HR			

23	Employees	To conduct exit interviews	Name, reasons for departure, opinions about the employer organisation. This record may be anonymous / pseudonymous	Legitimate interests (to gather information about reasons that employees depart and their opinion on the employer organisation)		HR			

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
1	All persons who visit the CCSP premises; authorised users of the CCTV system; persons to whom recordings/images are released	CCTV system. To protect the security of persons, property and the premises; to improve and provide information relating to health and safety matters; to facilitate investigations into serious incidents under College policies; to facilitate investigations into serious accidents under College policies; disciplinary matters involving employees and learners of Carlow College.	CCTV recordings and still images taken from the system; information recorded in the CCTV access log	Legitimate interests (CCTV helps to create a safe and secure environment); legal obligation		Authorised users (as defined in the CCTV Policy)	e.g. Gardai or other law enforcement; CCTV provider (Netwatch)		
2	All persons who sign in at Reception	To record details of visitors for health and safety purposes, and to record vehicle details for car park administration	Name, company (if relevant), times in and out, date, vehicle registration, name of employee visited	Legitimate interests (insurance, security, administration of facilities)		Reception, Fire Marshalls and Fire Wardens			
3	Learners, employees, Lennon House residents	Physical access control systems: car park barrier and automatic doors - to secure premises access; to verify that vehicles in car park are authorised	Name, photo, vehicle registration and details, phone number, date and time of barrier lift or door opening	Legitimate interests (security, car park administration)		Reception, Building Services	System provider		
4	Vehicle owners/drivers	To record and administer car parking violations and clamping	Vehicle registration	Legitimate interests (car park administration)		Building Services			
5	Any person identifiable/identified in report	Incident reports by security staff to highlight problematic incidents	Names, details of incidents	Legitimate interests (security)		Facilities Manager	An Garda Síochána		
6	Employees	To record use of keys for security purposes	Names, dates keys borrowed and returned	Legitimate interests (security)		Reception, Building Services			

No.	Data subjects	Purposes of Processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
1	Persons involved in accidents / incidents, witnesses, employees	To record and respond to reports of accidents, incidents and dangerous occurrences	Subject of accident / incident: name, date of birth, category of person (e.g. employee), injury and incident details, nature of treatment given, name of hospital / doctor sent to. If an employee was the subject of the accident / incident, whether PPE was needed and used, and number of working days missed. First aid responder: name. Witness: contact details. Employee: name of person responsible for any corrective measures	Legal obligation	Public interest	Health & Safety staff, Director of Operations	Health & Safety Authority		
2	Employees	Workstation assessments carried out for all purposes e.g. VDU, expectant mothers, remote working	Name, role, details of risk assessment, injuries, health risk	Legal obligation	Employment law	Health & Safety, HR			
3	Employees	To record details of training undertaken by employees for health and safety purposes	Name, nature of training, date training undertaken and expiry, if relevant	Legal obligation		Health & Safety			
4	Employees	To record the issuing of PPE to employees	Name, details of PPE which was issued	Legal obligation		Health & Safety			
5	Employees	Health surveillance records e.g. lead, carcinogens, ionising radiation (radon)	Medical reports,	Legal obligation	Employment law	Health & Safety			
6	Contractors	Contractor safety files	SafePass and related records	Legal obligation		Health & Safety			
7	Learners	To put in place and record personal evacuation plans in case of emergency	Name, contact details, details of plan	Legal obligation	Public interest	Health & Safety, Head of Student Services, designated assistant			

Building Services									
No.	**Data subjects**	**Purposes of processing**	**Categories of personal data**	**Article 6 legal basis**	**Article 9 legal basis**	**Internal users**	**Possible external recipients**	**Joint controller**	**3rd country transfer and safeguards**
1	Employees, residents	To respond to and record maintenance requests submitted to Building Services	Name, contact details, details of request	Contract, legitimate interests (to respond to requests for assistance)		Building Services, Facilities Manager			

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
1	Learners, employees, Governing Body members, third parties	Processing carried out for legal or statutory compliance purposes e.g. Charities Compliance, Data Protection, Freedom of Information, Health & Safety (see also Health & Safety section for further information), Safeguarding	Names, contact details, details of matter in hand	Legal obligation	Public interest	e.g. President's Office, Accounts, Data Protection Officer, Freedom of Information staff, Health & Safety staff, Director of Operations	e.g. Charities Regulator, Tusla, An Garda Siochana, Health & Safety Authority, Data Protection Commission, Office of the Information Commissioner		
2	Learners, employees, third parties	To obtain legal advice; for the establishment, exercise or defence of legal claims; to engage in legal cases	Details of events leading to advice being sought, or the establishment, exercise or defence of legal claims; advices	Legitimate interests (to administer legal matters), contract	Legal claims	President's Office, Director of Operations, any relevant function	Legal advisors		
3	Persons involved in incidents which may lead to claims, claimants	Notifying insurers of incidents, making claims	Details of incidents and claims	Legitimate interests (to defend and respond to incidents, claims)	S50, DPA 2018	Director of Operations, Facilities Manager	Insurance company		
4	Employees, learners, Governors, Trustees, other stakeholders	Meetings' records (i.e. committees, Programme Boards, policy sub-groups). To record College business	Names, details of matters under discussion and decisions made	Contract, legitimate interests (to record College business)		Members of the group in question; a summary version of minutes may be made available to staff at large	Validating body e.g. QQI		
5	Employees, other stakeholders	Records of team meetings. To record College business	Names, details of matters under discussion and decisions made	Contract, legitimate interests (to record College business)		Team members			
6	Correspondents, including the general public	General queries that do not fit under any other heading	Names, contact details, details of query	Legitimate interests (to deal with College business)		Reception, Student Recruitment Office (contact form on website), relevant staff			

7	Persons with whom employees have meetings	Appointment diaries	Names, contact details, reason for meeting	Legitimate interests (to deal with College business)		Diaries may be shared with administrative staff			
8	Correspondents	To record and respond to complaints and compliments	Names, contact details, details of complaint / compliments, reply	Legitimate interests (to deal with College business)		Relevant staff			
9	Individual making a protected disclosure, other involved individuals	To record and respond to protected disclosures	Names, contact details, details of protected disclosure, investigation records and report	Legitimate interests (to investigate and respond to protected disclosures)	Employment law	May include line manager, HR, Director of Operations, Protected Disclosures Group	May be reported to law enforcement, statutory or regulatory authorities; external investigator may be used		

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
1	Event organisers, registrants / attendees and speakers	To administer attendance at events	To the extent processed: names, contact details, organisation name	Contract; legitimate interests (to make name badges and/or registrant / attendee list available for networking purposes)		Event organiser	Attendees, speakers, booking platform providers (e.g Eventbrite), virtual platform (e.g. Zoom), any joint organiser		Eventbrite
2	Event registrants / attendees, speakers	To cater for special dietary requirements	Health / disability data, dietary requirements	Legal obligation	Consent	Event organiser	External provider e.g. caterer (if strictly necessary)		
3	Event organisers, registrants / attendees	To administer payments for events	Financial information	Contract		Event organiser, Facilities Manager, Accounts	Payments provider		
4	Event organisers, attendees and speakers	To create a photographic or film record of an event; for publicity and record purposes	Photographs or moving images/audio	Legitimate interests (to create a photographic / film record of an event; for publicity and record purposes); consent		Marketing & Student Recruitment Office	May be published on CCSP's social media and / or website		
5	Event invitees	To invite people to events	Name, contact details, invitation and reply	Legitimate interests (to invite guests to events)		Event organiser			
6	Attendees, speakers	Administration of virtual events, making recordings of virtual events available	To the extent processed: screen name, chat posts, questions asked, image, spoken contributions, device information	Legitimate interests (to make events and recordings available to a wide audience)		Event organiser, Marketing Office, Student Recruitment Office	Recordings may be published on the world wide web		
7	Mailing list members	To make event information available or other College information e.g. services, programmes	To the extent processed: name, contact details, marketing preferences, consent, withdrawal of consent	Consent, legitimate interests (to make event information available to current learners and employees, and any other individuals on mailing lists		Marketing Office, Student Recruitment Office, any other mailing list administrator			Mailchimp (USA): Standard Contractual Clauses

				processed 8under legitimate interests)					
8	Employees, learners	Creation of and making available College promotional materials in all formats e.g. prospectus, brochures, advertisements, video/audio footage website	To the extent processed: photographs, video / audio recordings, profiles, consent forms	Consent		Marketing Office, Student Recruitment Office	External service providers e.g. photographers, videographers		
9	Employees	Staff newsletter	Names, photographs, profiles	Legitimate interests (to make information available to staff)		Marketing Office, President's Office, all staff			
10	All website and platform users	Cookies and analytics on website and other platforms	Online identifiers	Consent (cookies); legitimate interests (to monitor use of platforms and website)		Marketing Office	Google Analytics, cookie owners		

Accommodation									
No.	**Data subjects**	**Purposes of processing**	**Categories of personal data**	**Article 6 legal basis**	**Article 9 legal basis**	**Internal users**	**Possible external recipients**	**Joint controller**	**3rd country transfer and safeguards**
1	Paying residents of Carlow College	To provide them with building and car park access; accommodation contract and records arising from it e.g. inspection records	Name, photo, access records, contact details, application, contract and related records	Contract		Reception, Facilities Manager, International Officer	US partner colleges, Security company		Standard Contractual Clauses
2	Guests of Carlow College	May vary depending on context: e.g. to provide them with accommodation services; to provide them with building and car park access	Name, photo, access records, contract, contact details, details of their stay	Legitimate interests (to provide accommodation to guests), contract		Reception, Facilities Manager, President's Office			

Section 2: Carlow College, St Patrick's as a Processor

No.	Data subjects	Purposes of processing	Categories of personal data	Article 6 legal basis	Article 9 legal basis	Internal users	Possible external recipients	Joint controller	3rd country transfer and safeguards
1	Learners (grant holders)	To administer matters relating to SUSI grants	Names, contact details, SUSI application number, PPSN, CAO number, date of birth, details of programme and stage, rates, free fees eligibility, registration status.	Public interest	Public interest	Grants staff (Admissions Office), Accounts	SUSI		

Appendix 3: Data Protection and IT Supplier Assessment Form

COLÁISTE CHEATHARLACH NAOMH PÁDRAIG
CARLOW COLLEGE ST. PATRICK'S

DATA PROTECTION AND IT SUPPLIER ASSESSMENT FORM

Purpose

This form is used to conduct due diligence on potential suppliers to Carlow College, St Patrick's (CCSP) where either personal data or a technology service is involved. Its purposes are to ascertain both how CCSP will use supplier services and the technical and organisational measures that the supplier has implemented to keep data safe.

Choosing a supplier

Adherence to the following measures simplifies assessments considerably:

- If personal data is involved, choose a supplier who is based in and stores data in the EU/EEA/Adequacy Decision country.[2]
- Choose a supplier who can supply CCSP with a contract, including data protection clauses.

Completing and submitting the form

1. Conducting an assessment can involve considerable work. This form is only to be submitted when a manager wishes to recommend a particular supplier. If you are at the stage of comparing suppliers, you may contact the Data Protection Officer (DPO) and/or the IT Department to discuss them.
2. This form must be submitted by the line or senior manager whose business area will be the main user of the supplier's services.
3. The following sections are to be completed:

Section A	All applicants

[2] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [accessed, 10 October 2023].

Section B	Technology product involved
Sections C and D	Personal data involved
Section E	Any applicant who wishes to provide further information

4. You may need to ask the supplier for documentation or information to answer some questions. You may either insert a link in the form to online documentation or send it to the Data Protection Officer.
5. If you have difficulty completing the form, please contact the DPO and/or the IT Department.
6. The form should be submitted by at least 10 working days before a decision is required. Complex arrangements and/or contracts that require Management Board approval may unavoidably have a longer turnaround time. Incomplete applications cannot be processed.
7. Send the completed form to: dataprotection@carlowcollege.ie.

Assessment process

The DPO, IT Department and/or Director of Strategy and Operations may contact the applicant requesting further information.

Supplier Assessment Form

Section A: Background information		
1	Name of manager submitting form	
2	If different, name of person who completed form	
3	Description of proposed services provided to CCSP	
4	Intended length of contract	
5	Name the CCSP function(s) that will use the services	
6	Will learners use the services?	Yes ☐ No ☐
7	Does the supplier provide a contract e.g. terms of service, service level agreement etc.?	Yes ☐ No ☐ If yes, provide a copy
8	Confirm that the supplier's services fulfil CCSP's business requirements	Yes ☐ No ☐
9	Confirm that you have read the supplier's terms and conditions and that CCSP can abide by them	Yes ☐ No ☐
10	Date by which decision on application is required	
Section B: Technology products		
11	Name of software / service / digital tool	
12	Approximate number of users	
13	If relevant, programmes and modules for use	
Section C: Data protection		
14	Who are the data subjects? [Data subject are the people the data is about].	Tick all applicable categories: CCSP employees ☐ CCSP job applicants ☐ CCSP registered learners ☐ CCSP prospective learners ☐ Other (explain) ☐
15	What CCSP personal data will be processed by the supplier?	Tick all applicable categories: Name, surname and/or date of birth ☐ Contact details (phone number, email address, postal address, Eircode) ☐ Official identification data (e.g. PPSN, passport number) ☐ Identification or access information (e.g. user name, password, reference number) ☐ Social media profile ☐ Economic and financial data ☐

		Location data (e.g. GPS) ☐ Photo, video or audio recordings ☐ Data relating to personal activities or family life ☐ Data relating to professional activities ☐ Education data ☐ Pseudonymised data ☐ Online identifier(s) e.g. IP address, device details ☐ Other (explain) ☐
16	Will special category personal data or criminal offence data be processed by the supplier?	Yes ☐ No ☐ If yes, tick all applicable categories: Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Genetic data ☐ Biometric data ☐ Health ☐ Sex life or sexual orientation ☐ Criminal offence data (including vetting) ☐
17	Who provides the data to the supplier?	Tick all applicable answers: Provided by CCSP ☐ Provided by data subjects ☐ Combination of (a) and (b) ☐ Other (explain) ☐
18	How will data be sent to the supplier? [e.g. secure file transfer, entered directly into supplier's system]	
19	Will the data be given to the supplier in plain text, pseudonymised or anonymised?	
20	How often is data given to the supplier?	Once-off ☐ Periodic (e.g. once a year) ☐ Numerous and continuous for the duration of the contract ☐
21	In relation to data protection roles and responsibilities, does the supplier consider itself a data processor and CCSP the data controller for any CCSP personal data processed by the supplier in the	Yes ☐ No ☐

	course of CCSP using the supplier's services?	
22	In which country(ies) will CCSP personal data be stored?	
23	If data is transferred to a country(ies) outside the EU/EEA//Adequacy Decision countries, what safeguards are in place?	Tick all applicable answers: A US entity covered by the Data Protection Framework (DPF) ☐ Standard Contractual Clauses ☐ Binding Corporate Rules ☐ Other (name) ☐ Provide a copy of the safeguards document
24	If Yes is the answer to Question 23, and the supplier is a US entity not covered by the Data Protection Framework (DPF), a Transfer Impact Assessment (TIA) is required. Does the supplier have a TIA?	Yes ☐ No ☐ If yes, provide a copy
25	Does the supplier outsource any part of the services provided to CCSP to sub-processors?	Yes ☐ No ☐ If yes, provide names and addresses of sub-processors and details of the services provided
26	Will CCSP data be shared with the supplier's parent or group companies?	Yes ☐ No ☐ If yes, described what CCSP data will be shared and for what purpose
27	Does the supplier have a Data Protection Officer?	Yes ☐ No ☐ If yes, provide contact details.
28	Does the supplier maintain records of processing activities?	Yes ☐ No ☐
29	Can the supplier provide a statement stating they feel they comply fully with the requirements of the GDPR?	Yes ☐ No ☐ If yes, provide a copy
30	Does the supplier provide a data processing agreement or clauses?	Yes ☐ No ☐ If yes, provide a copy
31	Does the supplier have a Privacy Notice(s)?	Yes ☐ No ☐ If yes, provide a copy
32	Does the supplier have a Data Protection Policy?	Yes ☐ No ☐ If yes, provide a copy
33	Does the supplier have a records retention schedule that covers CCSP personal data?	Yes ☐ No ☐ If yes, provide a copy
Section D: Supplier security information and documentation		
34	Does the supplier have a Technical Security Policy or similar document?	Yes ☐ No ☐ If yes, provide a copy

35	Does the supplier provide data protection and IT security training to its employees?	Yes ☐ No ☐
36	Do the supplier's employees sign confidentiality agreements that apply during and post-employment?	Yes ☐ No ☐
37	Has the supplier's data centre(s) achieved any security accreditation e.g. SOC2, SOC3?	Yes ☐ No ☐ If yes, provide a copy
38	Has the supplier achieved any security accreditation e.g. ISO 27001?	Yes ☐ No ☐ If yes, provide a copy
Section E: Other information		
39	Any other information you wish to provide	
Office Use Only		
40	Date form received	
Section F: IT Department		
41	Cost and duration of licences / subscriptions	
42	Details of known security incidents affecting the services in the past three years; list personal data breach incidents or cases of the product shipping with potentially unwanted applications (PUAs) bundled in an update.	
43	Support agreement (provide details)	
44	What training and/or support material is available?	
45	What monitoring / management tools are available as part of the software/service?	
46	Comments and queries. Include any details of expected issues with installation/rollout for new products. For products being renewed, include any concerns or issues encountered during use period.	
47	Recommendation on application	Yes ☐ No ☐ Explain rationale
Section G: DPO		
48	Comments and queries	
49	Recommendation on application	Yes ☐ No ☐ Explain rationale
Section H: Director of Strategy and Operations		
50	Decision	Yes ☐ No ☐

		Explain rationale
51	Complete if referred to Management Board for approval of expenditure	Decision: Yes ☐ No ☐ Explain rationale
52	Date decision communicated to applicant	

Document control

Version: 1.0

Appendix 4: Template Data Processing Agreement

CARLOW COLLEGE, ST PATRICK'S

AND

[PARTY 2]

DATA PROCESSING AGREEMENT

THIS AGREEMENT (herein defined as the "Agreement") is dated [date]

and entered into between:

1. **Carlow College, St Patrick's** having its registered office at College Street, Carlow, Co. Carlow, R93 A003 (hereinafter **"Controller"**)

-and-

2. **[PARTY 2]** having its registered office at [address] (hereinafter **"Processor"**)

BACKGROUND:

The Controller and the Processor are parties to an ongoing agreement [name and date of service agreement goes here], the "Service Agreement," for the provision of a [to be defined] service from the Processor to the Controller. In connection with the Service Agreement, certain Personal Data concerning Data Subjects (both as defined below) may be transferred from the Controller to the Processor. This Agreement is intended to govern such transfers.

DEFINITIONS:

For the purposes of this Agreement:

"**Applicable Data Protection law"** means any EU and Irish law which may apply to the terms of this Agreement and which may vary from time to time;

"Controller" and "Processor" shall have the meanings as set out in Article 4(7) and (8) respectively of EU General Data Protection Regulation 2016/679 (the "GDPR");

"Data Protection Commission" (DPC) is the supervisory authority for the purposes of Article 51 of the GDPR;

"Data Subject" means an individual who is the subject of Personal Data;

"Personal Data" shall have the meaning set out in Article 4(1) of the GDPR;

"Personal Data Breach" shall have the meaning set out in Article 4(12) of the GDPR;

"Prompt Notice" shall mean 24 hours unless otherwise expressly stated in this agreement;

"Special Category Data" shall have the meaning set out in Article 9(1) of the GDPR;

"Third Country" shall mean a location outside of the European Economic Area (EEA), the EEA being: Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

This Agreement, including these definitions and its recitals and schedules, is a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the data processing (as well as the Personal Data covered) are specified in Schedule 1 hereto.

WHEREAS:

Under the GDPR, a written Data Processing Agreement must be in place between the Controller and any organisation which processes personal data on its behalf, governing the processing of the data. This Agreement is intended to satisfy that obligation.

TERMS

The parties agree that:

1.1 The Controller and the Processor acknowledge that for the purposes of the Applicable Data Protection Law (as amended) Carlow College, St Patrick's is the Controller and **[PARTY 2]** is the Processor in respect of any Personal Data.

1.2 The Processor shall process Personal Data only for the purposes of carrying out their obligations arising under the Service Agreement.

1.3 The Controller shall instruct the Processor to process the Personal Data in any manner that may reasonably be required in order for the Processor to carry out the processing in compliance with this Agreement and Applicable Data Protection law.

1.4 The Controller shall refrain from providing instructions which are not in accordance with applicable laws including Applicable Data Protection law, and, in the event that such instructions are given, the Processor is entitled to resist carrying out such instructions.

1.5 The details of the transfer and of the Personal Data are specified in Schedule 1. The parties agree that Schedule 1 may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required by law. The parties may execute additional annexes/schedules to cover additional transfers, or may include multiple transfers in Schedule 1, which will be submitted to the DPC where required.

1.6 This Agreement shall continue for no less a term than the term of the Service Agreement.

1.7 The rights and obligations of the parties with respect to each other under this Clause 1 shall survive any termination of the Agreement.

2. REGULATORY COMPLIANCE

2.1 To the extent required by law or regulation:

2.1.1 The Processor shall co-operate with the DPC in connection with any activities performed by the Processor;

2.1.2 The Controller, its auditors and the DPC shall have effective access to data related to such activities, as well as effective access to the Processor's business premises;

2.1.3 The DPC shall have without notice the right of access to the Processor's business premises for purposes for this Clause 2; and

2.1.4 The Processor shall give prompt notice to the Controller of any development that may have a material impact on the Processor's ability to perform services effectively under this Agreement and in compliance with applicable laws and regulatory requirements.

3. OBLIGATIONS OF THE CONTROLLER

The Controller warrants and undertakes that:

3.1 The Personal Data has been collected, processed and transferred in accordance with the GDPR and all Applicable Data Protection law.

3.2 It has used reasonable efforts to determine that the Processor is able to satisfy its legal obligations under this Agreement.

3.3 It will respond to enquiries from Data Subjects and the DPC concerning processing of the Personal Data by the Controller, unless the parties have agreed that the Processor will so respond, in which case the Controller will still respond to the extent reasonably possible and with the information reasonably available to it if the Processor is unwilling or unable to respond. Responses will be made within a reasonable time and in accordance with the Applicable Data Protection law.

3.4 It will make available, upon request, a copy of this Agreement to Data Subjects who are relevant to the processing, the subject matter of this Agreement, unless this Agreement contains confidential information, in which case it may redact such information. The Controller shall abide by a decision of the DPC regarding access to the full text of this Agreement by Data Subjects, as long as Data Subjects have agreed to respect the confidentiality of the confidential information removed. The Controller shall also provide a copy of this Agreement to the DPC where required.

4. OBLIGATIONS OF THE PROCESSOR

The Processor warrants and undertakes that:

4.1 It will comply with all applicable law including Applicable Data Protection law in its performance of this Agreement.

4.2 It will only process the Personal Data on the instructions of the Controller.

4.3 It will not transfer Personal Data to a Third Country without the prior written approval of the Data Controller and only then once the transfer to the Third Country has been legitimised and the Controller and the Processor are satisfied that an adequate Data Protection regime exists in the Third Country.

4.4 It will not appoint sub-processors to process the Personal Data on its behalf without the prior written approval of the Controller.

4.5 Once approved by the Controllers, sub-processors will only process the Personal Data on the instructions of the Processor and the Processor will put in place a legal agreement in writing to govern the sub-processing.

4.6 It will have in place appropriate technical and organisational measures, and all measures pursuant to Article 32 of the GDPR, to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

4.7 It will obtain guarantees from any sub-processors processing the Personal Data, that they will have in place appropriate technical and organisational measures, and all measures pursuant to Article 32 of the GDPR, to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

4.8 It will have in place procedures so that any individual party it authorises to have access to the Personal Data, including employees of the Data Processor, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the authority of the Processor shall be obligated to process the Personal Data only on instructions from the Processor. This provision does not apply to persons authorised or required by law or regulation to have access to the Personal Data.

4.9 It will not disclose any Personal Data to a third party in any circumstances other than at the specific written request of the Controller, unless such disclosure is necessary in order to fulfil the obligations of the Service Agreement, or is required by applicable law.

4.10 It will notify the Controller of any request for information by the DPC and will not disclose any Personal Data without the prior consent of the Controller.

4.11 It will notify the Controller of any complaint, notice or communication received which relates directly or indirectly to the processing of the Personal Data, or other connected activities, or which relates directly or indirectly to the compliance of the Processor and/or the Controller with relevant applicable law including Applicable Data Protection law.

4.12 It will give the Controller prompt notice of a Personal Data Breach or a potential Personal Data Breach, once becoming aware of same, and the Processor will cooperate with the Controller in implementing any appropriate action concerning the breach or the potential breach as the case may be, including corrective actions.

4.13 It will delete from its systems all soft copies of any Personal Data and return all soft and hard copy documentation on the completion of the Service Agreement or on request from the Controller and will do so in a timely manner, giving a written confirmation of same having been done. The only exception to this Clause 4.14 shall be where the Processor shall have a legitimate reason, which is confirmed by the Controller, to continue to process particular data or where it is legally required to maintain data records.

4.14 Without prejudice to other legal provisions concerning the Data Subject's right to compensation and the liability of the parties generally, as well as legal provisions concerning fines and penalties, the Processor will carry full liability in the instance where it or its sub-processor is found to have infringed applicable law including Applicable Data Protection law through his processing of the Personal Data.

4.15 It has no reason to believe, at the time of entering into this Agreement, of the existence of any reason that would have a substantial adverse effect on the guarantees provided for under this Agreement, and it will inform the Controller (which will pass such notification on to the DPC where required) if it becomes aware of any such reason.

4.16 It will process the Personal Data for purposes described in Schedule 1, and has the legal authority to give the warranties and fulfil the undertakings set out in this Agreement.

4.17 It will identify to the Controller a contact person within its organisation authorised to respond to enquiries concerning processing of the Personal Data, and will cooperate in good faith with the Controller, the Data Subject and the DPC concerning all such enquiries within a reasonable time.

4.18 It will register with the DPC in accordance with the Applicable Data Protection law and do all things necessary to comply with the Applicable Data Protection law and be responsible in

accordance with law, both statutory and common law to Data Subjects for any infringement of privacy or disclosure arising from its negligence, howsoever caused.

4.19 It will be capable of demonstrating its compliance with the obligations of Applicable Data Protection law.

5. RIGHT OF AUDIT

5.1 Upon reasonable request of the Controller, the Processor will submit, and/or as appropriate its sub-processors will submit, data processing facilities, data files and documentation used for processing, reviewing, auditing and/or certifying by the Controller (or any independent or impartial inspection agents or auditors, selected by the Controller and not reasonably objected to by the Processor) to ascertain compliance with the warranties and undertakings in this Agreement, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Controller.

6. DATA SUBJECT RIGHTS

The Processor will assist the Controller, whenever reasonably required, in so far as possible, to fulfil the Controller's obligation to respond to requests for exercising Data Subject rights as provided under Applicable Data Protection law and the Processor will have the appropriate organisational and technical measures in place to deal with Data Subject requests.

7. LIABILITY AND INDEMNITY

7.1 The Processor will not be liable for any claim brought by a Data Subject arising from any action by the Processor to the extent that such action resulted directly from the Controller's instructions.

7.2 Except as provided for in Clause 7.1, the Processor shall indemnify the Controller for any monetary fine or penalty imposed on the Controller by the DPC that results from the Processor's breach of its obligations under this Agreement.

7.3 In the event that any claim is brought against the Controller by a Data Subject arising from any action by the Processor, to the extent that such action did not result directly from the Controller's instructions, the Processor shall indemnify and keep indemnified and defend at its own expense the Controller against all costs, claims, damages or expenses incurred by the Controller or for which the Controller may become liable due to any failure by the Processor or its directors, officers, employees, agents or contractors to comply with any of its obligations under this Agreement.

7.4 In the event that any claim is brought against the Processor by a Data Subject arising from any action or omission by the Processor to the extent that such action or omission resulted directly from the Controller's instructions, the Controller shall indemnify and keep

indemnified and defend at its own expense the Processor against all costs, claims, damages or expenses incurred by the Processor for which the Processor may become liable due to any failure by the Controller or its directors, officers, employees, agents or contractors to comply with any of its obligations under this Agreement.

7.5 Either party will provide the other party with evidence of financial resources to confirm it has sufficient such resources to fulfil its responsibilities under Clause 7.3 and 7.4 as appropriate (which may include proof of insurance cover).

8. LAW APPLICABLE TO THIS AGREEMENT

This Agreement shall in all respects be governed by and interpreted in accordance with the laws of the Republic of Ireland. The parties hereto hereby submit to the exclusive jurisdiction of the Irish Courts for all the purposes of this Agreement.

9. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE DPC

9.1 In the event of a dispute or claim brought by a Data Subject or the DPC concerning the processing of the Personal Data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

9.2 The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the DPC. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

9.3 Each party shall abide by a decision of the DPC which is final and against which no further appeal is possible.

10. TERMINATION

10.1 In the event that either the Processor or the Controller is in breach of its obligations under this Agreement, then either the Data Processor or the Data Controller may temporarily suspend the transfer of Personal Data to the Processor until the breach is repaired or the Agreement is terminated.

10.2 In the event that:

10.2.1 the transfer of Personal Data to the Processor has been temporarily suspended by the Controller for longer than one month pursuant to paragraph 10.1;

10.2.2 compliance by the Controller with this Agreement would put it in breach of its legal or regulatory obligations in the country of import;

10.2.3 the Processor or Controller are in substantial or persistent breach of any warranties or undertakings given by it under this Agreement;

10.2.4 a final decision against which no further appeal is possible of a competent court or of the DPC rules that there has been a breach of this Agreement by the Controller or the Processor; or

10.2.5 a petition is presented for the administration or winding up of the Controller, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Processor is an individual; a company voluntary arrangement is commenced by it;

or any equivalent event in any jurisdiction occurs,

then the Controller, without prejudice to any other rights which it may have against the Processor, shall be entitled to terminate this Agreement, in which case the DPC shall be informed where required.

10.3 The parties agree that the termination of this Agreement at any time, in any circumstances and for whatever reason (except for termination under Clause 10.2) does not exempt them from the obligations and/or conditions under this Agreement as regards the processing of the Personal Data transferred.

11. VARIATION OF THIS AGREEMENT

The parties may not modify this Agreement except to update any information in Schedule 1, in which case they will inform the DPC where required. This does not preclude the parties from adding additional commercial clauses where required and does not affect the Service Agreement between the Controller and the Processor. In cases where any conflict arises in the interpretation of these agreements, this Agreement shall take precedence.

SCHEDULE 1

DESCRIPTION OF THE TRANSFER

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects:

[To be inserted]

Purposes of the transfer(s)

The transfer is made for the following purposes:

[To be inserted]

Categories of data

The Personal Data transferred concern the following categories of data,
Personal Data and Special Category Data, including without limitation:

[To be inserted]

Recipients

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients: [To be inserted]

Contact point for data protection enquiries and to report a Personal Data Breach:

Controller

Telephone: 059-9153200

Email: dataprotection@carlowcollege.ie

EXECUTED by the parties on the date appearing at the top of page 1.

SIGNED

By:

Duly authorised for and on behalf of

the Controller

SIGNED

By:

Duly authorised for and on behalf of

the Processor

Appendix 5: Collaborations with External Partners: Data Protection Assessment Form

COLÁISTE CHEATHARLACH NAOMH PÁDRAIG
CARLOW COLLEGE ST. PATRICK'S

Collaborations with External Partners: Data Protection Assessment Form

Background information

1. Personal data may be shared between Carlow College, St Patrick's (CCSP) and external partners in the course of collaborative initiatives. A data sharing agreement may be needed. The purpose of this form is to gather information about collaborations. It will be used by the DPO as an assessment tool for data protection arrangements.
2. This form is not to be used where CCSP is contracting a supplier to carry out a service on its behalf. Instead, use the Supplier Assessment Form.

Completing the form

1. The Collaboration Lead is responsible for ensuring that the DPO is notified about discussions with an external partner as early as possible. The questions on this form may be used to guide discussions with the external partner and the DPO. **Do not wait until everything is agreed with the external partner to contact the DPO.** Late notification to the DPO may result in agreed measures having to be re-negotiated to comply with Data Protection law, so it is to your benefit to involve the DPO as early as possible. You do not need to have an answer to every question on this form to involve the DPO.
2. **This is an internal CCSP document and is for completion by CCSP staff only**. You may need to ask your external partner for documentation or information to answer some questions. If you require assistance completing the form, please contact DPO, CCSP.
3. Send your form and any documents necessary to understand it (e.g. process documents, agreements, learner information packs, policies of the external partner etc) to the DPO.
4. Notify changes to information recorded on this form to the DPO by updating this form. Changes to your process documents, agreements etc may cause changes to data protection arrangements.
5. Send this form to the DPO at least 10 working days prior to requiring a reply from the DPO.

Collaborations with External Partners: Data Protection Assessment Form

Step 1: Background information	
Name of person completing this form	
CCSP Collaboration Lead	
Step 2: Collaboration information	
What is the name of your collaboration?	
Explain what your collaboration is about	
Name the external partner(s)	
What is the role of CCSP in the collaboration?	
What is the role of the external partners(s) in the collaboration?	
Does the external partner(s) have a DPO?	Yes ☐ No ☐ If yes, provide name and email address:
Step 3: Personal data transfers	
Step 3A: Data transfers from CCSP to external partner(s)	
Does CCSP need to transfer personal data to an external partner(s)?	Yes ☐ No ☐
What is the purpose(s) of the data transfer?	
Is learner data involved?	Yes ☐ No ☐ If yes, tick all applicable categories: Name ☐ Date of birth ☐ Postal address or Eircode ☐ Personal email address ☐ CCSP email address ☐ Phone number ☐ Student ID No. ☐ Gender ☐ Personal photograph ☐ Academic grades / broadsheets ☐ Disciplinary information ☐ Deferral / withdrawal from programme ☐ Financial data ☐ Other (specify data types) ☐
Is learner special category or criminal offence data involved?	Yes ☐ No ☐ If yes, tick all applicable categories: Racial or ethnic origin ☐

	Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Health (includes learning differences, disabilities) ☐ Biometric data ☐ Genetic data ☐ Criminal offence data (including vetting) ☐
If learner data is involved, which institution are learners registered with?	Tick all categories that apply: Not applicable ☐ CCSP ☐ SETU (Carlow Campus) ☐ Both CCSP and SETU (Carlow Campus) ☐ Another institution (provide name) ☐
Is staff data involved?	Yes ☐ No ☐ If yes, list data types:
Is staff special category or criminal offence data involved?	Yes ☐ No ☐ If yes, tick all applicable categories: Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Health (includes learning differences, disabilities) ☐ Genetic or biometric data ☐ Criminal offence data (including vetting) ☐
If staff data is involved, who is the employer?	Tick all categories that apply: CCSP ☐ External partner(s) ☐ Other ☐ (specify employer name):
Is the personal data of any other data subject involved e.g. members of the public, External Examiner, event participants, children (under 18), research participants, vulnerable people? Note: vulnerable individuals may be, for example, mentally ill persons, asylum seekers, the elderly or patients etc.	Yes ☐ No ☐ If yes, provide further information:
Will the personal data be transferred to any location outside the European Economic Area?	Yes ☐ No ☐ If yes, explain what mechanism is proposed to be used:
Step 3B: Data transfers from external partner(s) to CCSP	
Does an external partner(s) need to transfer personal data to CCSP?	Yes ☐ No ☐

What is the purpose(s) of the data transfer?	
Is learner data involved?	Yes ☐ No☐ If yes, tick all applicable categories: Name ☐ Date of birth ☐ Postal address or Eircode ☐ Personal email address ☐ CCSP email address ☐ Phone number ☐ Student ID No. ☐ Gender ☐ Personal photograph ☐ Academic grades / broadsheets ☐ Disciplinary information ☐ Deferral / withdrawal from programme ☐ Financial data ☐ Other (specify data types) ☐
Is learner special category or criminal offence data involved?	Yes ☐ No ☐ If yes, tick all applicable categories: Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Health (includes learning differences, disabilities) ☐ Genetic or biometric data ☐ Criminal offence data (including vetting) ☐
If learner data is involved, which institution are learners registered with?	Tick all categories that apply: CCSP ☐ SETU (Carlow Campus) ☐ Both CCSP and SETU (Carlow Campus) ☐ Another institution (provide name) ☐
Is staff data involved?	Yes ☐ No ☐ If yes, list the types of data:
Is staff special category or criminal offence data involved?	Yes ☐ No ☐ If yes, tick all applicable categories: Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Health (includes learning differences, disabilities) ☐ Genetic or biometric data ☐

	Criminal offence data (including vetting) ☐
If staff data is involved, who is the employer?	Tick all categories that apply: CCSP ☐ External partner(s) ☐ Other ☐ (specify employer name):
Is the personal data of any other data subject involved e.g. members of the public, External Examiner, event participants, children (under 18), research participants, vulnerable people? Note: vulnerable individuals may be, for example, mentally ill persons, asylum seekers, the elderly or patients etc.	Yes ☐ No ☐ If yes, provide further information:
Will the personal data be transferred to any location outside the European Economic Area?	Yes ☐ No ☐ If yes, explain what mechanism is proposed to be used:
Step 3C: Questions applicable to all data transfers	
Is the data involved in the transfer plain text, pseudonymised, encrypted?	
How it is proposed to transfer data?	
Which CCSP office(s)/employee(s) are directly involved (send/receive) in data transfers?	
Explain the timing of the data transfer(s)	One-off ☐ Periodic ☐ Numerous and continuous ☐ Provide any other relevant information:
Is all the data you plan to transfer necessary to achieve your purpose?	Yes ☐ No ☐ (Explain your answer)
Would it be possible to reduce the amount of data involved?	Yes ☐ No ☐ (Explain your answer)
Are you complying with all relevant data protection laws? If you answer 'no' or 'don't know' the DPO will contact you for further information.	Yes ☐ No ☐ Don't know ☐
Would your use of the data be unethical, unlawful or contravene industry guidelines, codes of practice or best practice in any way?	Yes ☐ No ☐ Don't know ☐
How is it proposed to notify data subjects of the data transfer?	
Step 4: Questions about academic programme delivery only (skip to Step 5 if n/a)	
Which institution's quality assurance framework and policies apply?	CCSP ☐ SETU (Carlow Campus) ☐ Another higher education institution (specify) ☐

Which institution is administering learner admissions i.e. accepts and makes decisions on applications?	CCSP ☐ SETU (Carlow Campus) ☐ Another higher education institution (specify) ☐
Will a representative of CCSP or a partner(s) be a member of a partner's committee for this collaboration e.g. Programme Board?	Yes ☐ No ☐ If yes, explain
Who is appointing the External Examiner?	CCSP ☐ SETU (Carlow Campus) ☐ Both CCSP and SETU (Carlow Campus) ☐ Another higher education institution (specify) ☐
Who is responsible for making any required HEA returns?	CCSP ☐ External partner(s) ☐
Who is responsible for making any required returns to the Dept for Social Protection?	CCSP ☐ External partner(s) ☐
Step 5: Access to systems/facilities	
Will CCSP learners or staff have access to systems of the external partner(s) (e.g. VLE, library)?	Yes ☐ No ☐ If yes, list relevant systems:
Will learners registered only with an external partner or their staff have access to CCSP systems (e.g. VLE, library)?	Yes ☐ No ☐ If yes, list relevant systems:
Step 6: Final steps	
What assistance do you require from the DPO?	
Any other information you wish to provide	
Indicate whether this is the first version or a revised version of this form that you have submitted	First version ☐ Revised version ☐
Provide overview of revisions here	
By what date are finalised data protection arrangements needed for your collaboration?	

Note: send any documents necessary to understand this form with it (e.g. process documents, agreements, learner information packs, partner's policies).

Office Use	
Date received	
Comments/queries	
Date comments/queries sent	

Appendix 6: Data Subject Request Form

You can use this form, if you wish, to make a request under the GDPR or *Data Protection Act* 2018.

Section 1: Contact details

Please include details we can use to easily contact you if we need further information to process your request.	
Name	
Address	
Phone number	
Email address	

Section 2: What is your relationship to Carlow College, St Patrick's e.g. current learner?

Section 3: Your request

Which data protection right do you wish to exercise?	
Access ¨ Information ¨ Rectification ¨ Objection ¨	Restriction ¨ Erasure ¨ Data portability ¨ Automated processing and profiling ¨

Please provide details of your request in the box below, including a description of the relevant personal data. Please provide as much detail as possible. If your request is broad or unclear, we may need to contact you for further information.

Section 4: Identification

We need to verify your identify in order to process your request. Please include a copy of your identification document (e.g. passport, driver's licence, student ID card). Photo-identification may be required for visual records (e.g. CCTV) to correctly identify you. A copy of an identification document is usually sufficient, but we reserve the right to request access to original documents. Copies of identification will be destroyed securely once we have verified your identity.

Please confirm either Section 5 or Section 6, as appropriate.

Section 5: Declaration of data subject making a request on their own behalf

I confirm that I am the data subject named in Section 1. I understand that the information I have supplied will be used to confirm my identity and assist in locating data to respond to my request.	
Signed:	Date:

Section 6: Declaration of data subject for an agent to act on their behalf

If you wish someone else to submit a request and receive responses on your behalf (e.g. solicitor, family member), please complete this section.

I confirm that I am the data subject named in Section 1. I give permission for the person or organisation named below to act on my behalf in respect of my data subject request. I have enclosed evidence of my identity and confirm that I want all responses to my request to be sent to the person or organisation named below. I understand that the information I have supplied will be used to confirm my identity and assist in locating data to respond to my request.	
Signed:	Date:

Name of agent	
Name of organisation (if relevant)	
Address	
Phone number	
Email address	

Section 7: Returning your completed form

Please return your form and proof of identity to the Data Protection Officer by email to dataprotection@carlowcollege.ie or by post to: Data Protection Officer, Carlow College, St Patrick's, College Street, Carlow.

Office use only

Reference No.	
Data request received	
Identify verified	Yes/No
If yes: Copy ID Name of employee who verified and shredded ID	Yes/No

Original ID supplied in person	Yes/No
Original ID checked and returned to requester	Yes/No

Appendix 7: Template Data Protection Impact Assessment

Carlow College, St Patrick's

Data Protection Impact Assessment Template

DPIA Template[4]

Consult Data Protection Commission guidance prior to filling the DPIA.[5]

Step 1a: DPIA Screening Checklist		
Does your project involve:	**Yes**	**No**
Evaluation or scoring of personal data (including profiling and predicting) on which decisions are based that produce legal or other significant effects		
Processing on a large scale of special category data or data relating to criminal convictions or offences		
Systematic monitoring of a publicly accessible area on a large scale		
Use of personal data on a large scale for a purpose other than that for which it was originally collected		
Profiling vulnerable persons, including children, to target marketing or online services at such persons		
Use of profiling or algorithmic means or special category data to determine access to services or that results in legal or similarly significant effects		
Systematically monitoring, tracking or observing individuals' location or behaviour		
Profiling individuals on a large scale		
Processing biometric data to uniquely identify an individual or enable the identification or authentication in combination with any other criterion set out in WP29 DPIA Guidelines		
Processing genetic data in combination with any other criterion set out in WP29 DPIA Guidelines		
Indirectly sourcing personal data where GDPR transparency guidelines are not met, including when relying on exemptions based on impossibility or disproportionate effort		
Combining, linking or cross-referencing data sets where linking significantly contributes to or is used for profiling or behavioural analysis, particularly where the data sets are combined from different processing operations or different controllers		
Large scale processing of personal data where the Data Protection Act 2018 requires 'suitable and specific measures' to be taken in order to safeguard rights and freedoms of individuals		
If you have answered yes to any of the above questions, you must carry out a DPIA.		

[4] Adapted from https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

[5] https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#:~:text=A%20Data%20Protection%20Impact%20Assessment%20(DPIA)%20describes%20a%20process%20designed,demonstrating%20compliance%20with%20the%20GDPR.

Step 1b: Identify the Need for a DPIA

Explain broadly what the project aims to achieve and what type of processing of personal data it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA (this can draw on your answers to step 1a).

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 another way of describing data flows. 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?
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 has 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?

Step 3: Assessment of Necessity and Proportionality of Processing

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? Prior consultation?

Step 4: Consult with Stakeholders

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?

Step 5: Identifying Privacy Risks and Mitigating Measures

Risk ID	Describe the risk and nature of potential impact on individual		Risk Owner		Current CONTROLS (provide details of how you currently manage the risk)	Assessment of Risk			Describe what further ACTIONS you will take to reduce the Impact/Likelihood and mitigate the risk. State who is the risk owner for each action
						Impact (1,2,3,4,5)	Likelihood (1,2,3,4,5)	Score	

Step 7: Sign off and document DPIA Outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
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:		
Residual risks approved by:		If accepting any residual high risk, consult the Data Protection Commission before going ahead
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with the DPIA

Appendix 8: Personal Data Breach Response Plan

COLÁISTE CHEATHARLACH NAOMH PÁDRAIG
CARLOW COLLEGE ST. PATRICK'S

Personal Data Breach Response Plan

What is a personal data breach?

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

Internal notification

Any actual or suspected personal data breach, or that data has been placed at risk, is to be notified the DPO immediately. This includes a breach notification sent to Carlow College by any processor, joint controller or collaborative partner.

You must ensure that the DPO receives the information. If you do not succeed in contacting the DPO, contact the President's Office or the Director of Operations. Again, you must ensure that the information has been received.

Assessment of situation

An assessment into the circumstances of the reported breach will commence as soon as possible. The scale of an assessment will be influenced by the situation.

Normally, the assessment team will include the President, the Director of Operations and the DPO. Other employees may join the assessment team depending on the circumstances. The DPO will advise the assessment team.

The assessment team will determine:

- Whether a breach has occurred;
- The nature of the personal data involved (including whether it includes special categories of personal data);
- The cause of the breach;
- Establish whether there is anything that can be done to recover a loss or contain further loss. This may involve engaging the services of contractors/processors;
- The number of individuals who are affected;
- The potential risk to affected individuals.

The results of the assessment will determine what notifications and further actions are required, if any. Complex, large-scale breaches will require thorough investigation. An Garda Síochána will be notified in cases involving criminal activity.

Notifying a personal data breach to the Office of the Data Protection Commission (DPC)

Controllers have a mandatory obligation to report data breaches to their supervisory authority (the DPC) within 72 hours of becoming aware of a breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

When a controller notifies a breach to the DPC, it should, at the minimum:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- Communicate the name and contact details of the DPO or other contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The controller should also inform the DPC if it intends to provide more information at a later point. The DPC may request further details of part of its investigation into a breach. The DPC is empowered to require controllers to inform data subjects about the breach.

If notification is not made within 72 hours, a reasoned justification for the delay must be provided. The 72 hours does not take weekends, public holidays etc into account. Awareness begins when the controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

Notifying personal data breaches to data subjects

Controllers have to notify data subjects where the data breach is likely to result in a 'high risk' to affected data subjects. WP29 (now the European Data Protection Board; hereafter EDPB) advice is that 'high risk' exists when the breach may lead to physical, material or non-material damage for the individuals whose data has been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that involves racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offended or related security measures, the breach should be considered high risk.

Notification to data subjects is not required where:

- The controller has implemented appropriate technical and organisational measures that render the personal data unintelligible to anyone not authorised to access it, such as encryption; or
- The controller has taken subsequent measures which ensure that the high risk to data subjects is not likely to materialise; or

- It would involve disproportionate effort, in which case there should be a public communication instead.

In the event that Carlow College informs data subjects of a data breach, the most appropriate method will depend on the circumstances. In general, data subjects must be contacted by some personally directed method rather than a general public notice.

Notification may be by telephone call, SMS, email or letter. Public notices may also be posted on the College website or social media accounts.

When notifying data subjects of a breach, the controller should provide the following information, at least:

- A description of the nature of the breach;
- The name and contact details of the DPO or other contact point;
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where appropriate, specific advice should be given to data subjects to protect themselves from possible adverse consequences of the breach, such as resetting passwords where access credentials have been compromised.

At the request of the President, the Marketing Office may assist in communicating with data subjects and responding to any media queries.

Required actions when Carlow College is a processor

Carlow College is a processor in terms of some its data processing. Processors have to notify controllers of breach situations. WP29 (now the EDPB) guidance is that processors notify controllers immediately, with further information about the breach provided in phases as information becomes available. Notifications to controllers will be in writing.

The DPO will act as a point of contact for controllers at the request of Carlow College. Data sharing agreements may impose a timeframe for notification to controllers.

Review of response to breach

In the aftermath of a personal data breach, a review of the incident may take place to ensure both that the steps taken during the incident were appropriate and effective, and to identify any organisational or technical measures that require updating to minimise future risk of a similar incident.

Register of breaches

Controllers must keep an internal record of all data breaches, a description of the facts of the breach, its effects and the remedial action taken. The record should also include reasoning for decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers that the breach is unlikely to result in a risk to the rights and freedoms of individuals. The DPO will keep this record on behalf of Carlow College.

Appendix 9: Online Meetings and Events

COLÁISTE CHEATHARLACH
NAOMH PÁDRAIG
CARLOW COLLEGE
ST. PATRICK'S

Online Meetings and Events

Purpose

The purpose these guidelines is to inform members of the College community about appropriate video conferencing use and etiquette. The terms 'business meeting' and 'event' are used throughout. The term 'business meeting' refers to any meeting that concerns the official business of Carlow College, and 'event' might refer to conferences, lectures, colloquia, open days, information sessions etc. Events may be attended by the College community and/or invited guests, the general public.

Platforms

- Employees are to use Microsoft Teams for internal meetings.
- It may be more appropriate to use webinar than meeting settings for some events (e.g. public events), and Carlow College has a Zoom account that employees can avail of.
- Caution should be exercised when subscribing to any virtual platform, in particular, think about what permissions you are being asked for and whether they are necessary (e.g. your location; access to your contacts). The minimum information should be shared with platforms.
- Avoid sharing organisational data, document locations or hyperlinks when using any platform other than Microsoft Teams.

Your device

- Ensure that your device has the necessary updates, including operating system and software updates.
- Ensure that your device is protected by antivirus software.
- Be conscious of what and who can be seen and heard from your camera. Protect the privacy of other people around you.
- If screen sharing, ensure that confidential data is not visible on screen and choose settings to ensure that pop ups such as emails do not appear on screen.
- Ensure that that you log out of, mute your mic or turn off your camera (as appropriate) when leaving a meeting or taking a break from it.
- Consider the data protection and privacy rights of others before you share an image or video of a video call that includes the image, voice or contact details of participants. Such sharing is discouraged.

Recording business meetings

- In general, business meetings are not to be recorded, and where this is proposed, there should be an identified legitimate reason for recording, which should be notified in advance to all participants, as well as the intended uses and sharing of the recording.
- Covert recording refers to recording, audio or visual, carried out without the knowledge and consent of an individual(s). It includes devices and systems of all types, including but not limited to, CCTV, phones and virtual meeting platforms. Employees and learners are not permitted to carry out covert recording of employees, learners or any person with whom they come into contact in the workplace or through the course of their duties or studies. Any covert recordings must have the prior approval of a representative group of senior management.
- Inform participants when beginning/ending recording.
- Recordings should not be kept for longer than is necessary to fulfil the purpose for which they were created.
- Recordings are potentially accessible under Data Protection and Freedom of Information laws.

Recording events

- It may be proposed to record events and make the recording available online. In such cases, the recording and sharing is to be notified to participants when booking the event and to speakers when they are invited to participate. There should always be a legitimate reason for recording an event and sharing that recording, whether online or by some offline means.
- Recordings should be reviewed by the event organiser prior to sharing the recording or making it available online. Where special category data is disclosed by any participant or where there may be legal implications (e.g. defamation), the recording should be edited to redact the data or a decision made not to share or publish the recording should be taken.
- Recordings are potentially accessible under Data Protection and Freedom of Information laws.
- Recordings should not be kept for longer than is necessary to fulfil the purpose for which they were created.

Hosting events

- It is the responsibility of the event organiser to make data protection information to participants.
- Carlow College has an Events Privacy Notice, which should be made available to all participants at the time of booking (i.e. not after booking).
- The Events Privacy Notice should also be made available to proposed speakers when they are invited to participate in an event.
- The Events Privacy Notice is generic and cannot take account of details specific to individual events. Therefore, the event organiser should supplement the Events Privacy Notice with any required further information that should be provided (e.g. if it is proposed to record the event; or make the recording available on the internet). This further information should be made available at the same time as the Events Privacy Notice.

- Video conferencing platforms have various functionalities. Settings should be chosen to promote data security and data protection rights:
    - Restrict access to video calls to those who need to present. Do not publish meeting IDs or passwords.
    - If sensitive topics are being discussed, consider whether participants can ask questions anonymously. Do not mention the names of participants when answering their questions.
    - Mute participant mics and turn off participant cameras unless participants require such permissions.

Appendix 10: Privacy Notices

Privacy Notices are made available on the Data Protection section of the College website. Ensure that the website is checked for the latest version of Privacy Notices.

No.	Name
1	Athena Swan Privacy Notice
2	Employee Recruitment Privacy Notice
3	Events Privacy Notice
4	Learner FAQ and Privacy Notice: Online Teaching and Learning
5	Mailing Lists Privacy Notice
6	Privacy Notice for Employees
7	Privacy Notice for Learners
8	Privacy Notice for Members of the Governing Body
9	Privacy Notice for Research Participants
10	Accommodation Privacy Notice
11	Wi-Fi Privacy Notice

Appendix 11: Template for Legitimate Interests Assessment

COLÁISTE CHEATHARLACH NAOMH PÁDRAIG
CARLOW COLLEGE ST. PATRICK'S

Legitimate Interests Assessment

When you rely on the 'legitimate interests' legal basis of the General Data Protection Regulation (GDPR) to process personal data, you must carry out a Legitimate Interests Assessment (LIA). An LIA is a three-part test that involves: (1) identifying a legitimate interest (2) showing that the processing is necessary to achieve the legitimate interest and (3) balancing the legitimate interest against the data subject's interests, rights and freedoms. Guidance on legitimate interests from the Data Protection Commission is available here (pp22-24).

You can use this form to help assess whether legitimate interest can be applied to your processing of personal data. You should complete and keep a record of the LIA to provide justification for your decision to use legitimate interest as a legal basis before you start processing the data. Send a copy of the LIA to the Process Owner and the Data Protection Officer (DPO). All LIAs must be agreed by the Process Owner and DPO before data processing begins. If you cannot identify a legitimate interest, contact the DPO to discuss the proposed processing.

Process name / description	
Is the process listed in the ROPA?	Yes ☐ No ☐
ROPA Reference	
Nature of personal data processed	
Data subject(s)	
Special category, criminal offence or child/vulnerable person data?	Yes ☐ No ☐ [If yes, give further details]
Process Owner (listed in ROPA)	
Assessment Owner	
Assessment start date	

1) Purpose: identify the legitimate interest(s). Consider:	
Why do you want to process the data – what are you trying to achieve?	
Who benefits from the processing (e.g. data subject,	

controller, third party)? In what way?	
Are the legitimate interests of the third party aligned with the party who wants to rely on legitimate interests?	Yes ☐No ☐ [Explain your response]
Are there any wider public benefits to the processing?	Yes ☐ No ☐ [If yes, provide further detail]
How important are those benefits?	
What would the impact be if you couldn't go ahead?	
Would your use of the data be unethical, unlawful or contravene industry guidelines, codes of practice or best practice in any way?	Yes ☐ No ☐ [If yes, provide further detail]
Have you considered any case law, Data Protection case studies etc?	Yes ☐No ☐ [If yes, provide further detail]
Does any law or official guidance etc specifically identify the data processing as possessing a legitimate interest?	Yes ☐No ☐ [If yes, provide further detail]
2) Necessity: apply the necessity test. Consider:	
Does this processing actually help to further the identified legitimate interest?	Yes ☐ No ☐[Explain your response]
Is it a reasonable way to go about it?	Yes ☐ No ☐ [Explain your response]
Is there another less intrusive way to achieve the same result e.g. process less data? Can the scope of the data processing be reduced?	Yes ☐ No ☐ [If yes, provide further detail]
Does any other GDPR legal basis apply to the processing?	
3) Balancing: apply the balancing test. Consider:	
Is the data about people in their personal or professional capacity?	

What is your relationship with the data subject? Is it pre-existing and have you used their data previously?	
Is there a two-way relationship in place with the data subject?	
Did you collect the data directly from the data subject? What did you tell them about how it would be used at the time?	
If the data was supplied by a third party, what did they tell the data subject about reuse and does this cover you?	
How long ago was the data collected from the data subject?	
Do you have the means and processes to keep the information up to date?	Yes ☐ No ☐ [Explain your response]
Is any of the data particularly sensitive or private?	Yes ☐ No ☐ [If yes, provider further detail]
Would people expect you to use their data in this way?	Yes ☐ No ☐ [Explain your response]
Are you happy to explain it to them?	Yes ☐ No ☐ [If no, explain your response]
Are some people likely to object or find it intrusive?	Yes ☐ No ☐ [If yes, explain your response]
What is the possible impact on the individual? Is the processing likely to cause unwarranted harm or distress?	
How big an impact might it have on them?	
Can you adopt any safeguards and technical measures to minimise the impact?	Yes ☐ No ☐ [Explain your response]
Can you offer an opt-out?	Yes ☐ No ☐ Partly ☐ [Explain your response]

Decision	
Decision date	

Decision: Can you use legitimate interests to process the data?	Yes ☐ No ☐
How was the outcome decided?	
Further action	
Date of DPO agreement	
Date of Process Owner agreement	
Next review date	

Appendix 12: Guidelines on Surveys

COLÁISTE CHEATHARLACH NAOMH PÁDRAIG
CARLOW COLLEGE ST. PATRICK'S

Guidelines on Surveys

1. Scope and responsibilities

1.1 These guidelines apply to staff of Carlow College, St Patrick's using a survey for work purposes.

1.2 Surveys for academic purposes, including learner surveys and market research surveys for Programmes, are approved in principle by the Office of the Registrar. Staff surveys are approved in principle by Human Resources (HR). Staff responsible for the survey agree survey questions, data privacy information and a data management plan with the Data Protection Officer (DPO).

1.3 Each College survey must have a sponsoring line manager. This should be the line manager whose functional area is the sole or principal user of survey data. While the line manager may delegate responsibility for actions described below, the line manager is responsible for ensuring adherence to these guidelines. The sponsoring line manager is responsible for notifying any proposed changes to submitted documentation to relevant functions i.e. Office of the Registrar, HR and DPO.

1.4 These guidelines deal with SurveyMonkey and Microsoft Forms, survey platforms which are used in Carlow College.

1.5 Surveys are useful for gathering quantitative information. If complex qualitative information, such as personal experience is being collected, it is appropriate to use a different mechanism e.g. individual interview or focus group.

2. Definitions

Anonymous means that no individual can be identified from survey data, or survey data in conjunction with other data. Data protection law does not apply to anonymous information.

Pseudonymous personal data means that it may be possible to identify an individual from survey data, sometimes in conjunction with other data e.g. if a staff member answers survey questions about their age range, gender and department, it may be possible to identify them from an answer or a combination of their answers. If it is possible to identify individuals (either respondents or individuals mentioned in responses), data protection law applies to the survey.

3. Process for conducting surveys

1	Survey approval	The sponsoring line manager applies to the following functions on the Survey Approval Application Form (Appendix 1) for approval in principle to carry out a survey:

		• Office of the Registrar for academic surveys, including learner surveys and market research surveys for Programmes.[6] • HR for staff surveys.
2	Survey creation	The following items (Appendix 2) are drafted by staff responsible for the survey for agreement with the DPO: • Survey questions • Data privacy information • Data management plan Approval in principle must be in place prior to sending this documentation to the DPO. The approved Survey Approval Application Form should also be sent to the DPO. The DPO will consult as required, which may include the approving function(s).
3	Conduct pilot survey	Send the survey to a small number of staff or stakeholders to gather feedback and test it from various perspectives e.g. clarity of questions, identify errors and omissions, functionality (both questions and reporting tool) and that only expected information appears in the raw survey data. Pilot respondents should be instructed not to insert information about themselves as answers. A Test Collector can be set up in SurveyMonkey to preview (pilot) a survey. Data should be deleted after the preview has been completed.
4	Conduct survey	Survey is released to invited respondents.
5	Review raw survey data	This review is carried out by one staff member or a small group of staff with a view to editing (redacting/deleting) responses that may cause damage or distress. Editing should be appropriate to the survey in question. Some survey responses may continue to identify individuals e.g. lecturers are identifiable in module feedback surveys, and learners may compliment staff in surveys.
6	Conduct analysis	Analysis is carried out on survey data. This involves considering reports generated from survey data and may also involve creating accompanying written commentary. Analysis may be conducted by more staff than those who participated in Step 5. Analysis should incorporate reviewing the survey to ascertain if there are learnings for future surveys e.g. if questions have not been answered or responses are not complete, consider the complexity of questions.
7	Report on survey findings	Provide a report on survey findings and arising recommendations and actions to relevant functions.
8	Provide feedback	Provide feedback to survey respondents on survey findings and actions that will be taken.

[6] Carlow College has an annual calendar of learner surveys. Staff who wish to conduct an additional learner survey should apply to the Office of the Registrar as early as possible in the academic year and note that it is preferred to have only one survey live at any one time to reduce the possibility of low response rates.

9	Delete raw survey data	Delete raw survey data at the agreed time. This is normally stated in the data privacy information. Anonymous survey responses can be retained indefinitely.
10	Implement agreed actions	Implement agreed actions.

4. Data privacy information

4.1 Data privacy information should be given at the beginning of the survey. Respondents agree to take part on the basis of what they are told in data privacy information, and accuracy and transparency are important. Data privacy information should include the following:

- The purpose of the survey.
- The College function or staff that will use survey data.
- Survey data is not normally shared externally to Carlow College, but if this is to happen, the organisation/individual should be named in data privacy information.
- The College function, staff or committee to whom reports arising from the survey are given.
- The College function that is administering the survey.
- How long survey data will be retained.
- Whether and how feedback will be given to respondents.
- A working hyperlink to the relevant Carlow College Privacy Notice. The most usual Privacy Notices are those for learners and employees.
- A working hyperlink to the Privacy Notice of the survey platform e.g. SurveyMonkey and Microsoft Forms. If SurveyMonkey is used, the data privacy information must state that the survey data will be exported to the USA.
- Survey data should not normally be matched with other data, but if this is intended, it must be mentioned in the data privacy information.
- If it is intended that a survey is anonymous, respondents should be instructed not to insert identifying information about any individual, including themselves.

4.2 If a survey is completely anonymous, it is sufficient in data protection terms to simply state this fact, however, communicating the aforementioned information to potential respondents may encourage participation.

5. Other introductory information

5.1 Indicate how many minutes it typically takes to complete the survey.

5.2 Thank respondents for taking part and tell them why participation is important.

5.3 If it is intended to send follow up surveys in the future, offer an opt-out option to respondents by including a contact email address in the introductory information.

6. Children's data

6.1 Surveys are not to be sent to children under the age of 16 unless prior parental/guardian consent is in place.

7. Survey design and questions

7.1 It is good practice that the first survey question acquires respondent agreement for their data to be used as outlined in the data privacy information e.g. 'I agree to participate in this survey and for my data to be used as outlined in the supplied Data Privacy Information.' If technically possible, the survey questions should only be available to respondents who have agreed with this statement. If agreement is not granted, the responses should be deleted from raw survey data and not analysed.

7.2 Surveys should permit respondents to scroll back and forth through their responses and change them.

7.3 Do not collect respondent IP addresses. See 8.4 for relevant instructions.

7.4 Survey questions should only ask for information that is necessary for the identified purpose of the survey. Information that might be useful or interesting does not qualify as 'necessary' and it is inappropriate to mark such questions as optional and leave it to the respondent to decide how to respond.

7.5 Particular care should be taken not to ask for special category personal data unless strictly necessary. Special category personal data refers to: race/ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health data (including learning differences/disabilities), and data concerning sex life or sexual orientation. It has become common to ask about gender and ethnicity in surveys, however, if this information is not strictly relevant to the survey, do not ask for it.

7.6 Make identity questions as general as possible. People are less likely to answer honestly or participate if they feel they are identifiable e.g. staff surveys should normally categorise staff as 'academic' or 'professional services staff'; and include a 'prefer not to say' option in questions about age range, gender, ethnicity or other particularly private information.

7.7 Where possible, be inclusive when asking about gender and ethnicity by providing various options and including an 'other' field which respondents can complete as they wish e.g. gender options might be male, female, non-binary, other (state), prefer not to say.

7.8 General advice for composing questions is as follows[7]:

- In terms of question order, put straightforward questions towards the beginning of the survey with questions that require more thought following this.
- Word questions clearly.
- Think about the information that is needed and word questions in a way that elicits this information.
- If it may not be obvious to respondents why particular questions are being asked, this should be explained.

[7] https://www.surveymonkey.com/mp/survey-guidelines/ [accessed on 22 March 2023].

- Ask mostly closed-ended questions i.e. where respondents choose from multiple choice, likert scale or yes/no options etc. Narrative questions (which provide blank fields for respondents to complete as they wish) should be kept to a minimum (1-2 per survey).
- Include 'not relevant', 'don't know' or similar terms as possible answers, where appropriate.
- Keep answer choices balanced. Using answer choices that lean in a particular direction can result in inauthentic responses e.g. instead of offering 'very helpful', 'helpful' and 'neither helpful nor unhelpful' as answers, offer 'very helpful', 'helpful', 'neither helpful nor unhelpful', 'unhelpful' and 'very unhelpful'.
- Avoid using absolutes e.g. 'every', 'always' and 'all'. They force the respondent to agree or disagree with a strongly worded question instead of allowing more nuanced answers.
- Do not ask leading questions.
- Avoid questions that ask about more than one topic e.g. 'How would you rate your programme of study and our learner support services?' Either choose one topic to ask about or create two separate questions.
- Put identity questions at the end of the survey e.g. age range, gender identity.

7.9 Various 'Collector Types' are available in SurveyMonkey. 'Share a survey link' is that which is usually used.

8. Anonymity

8.1 By default, surveys are to be anonymous for respondents. No attempt should be made to identify respondents.

8.2 It can be difficult to achieve anonymity as it is sometimes possible to identify individuals from one or a combination of their answers. Supplied data privacy information must not promise anonymity if this is not the case.

8.3 Carlow College has relatively small staff and learner populations and reports generated from survey data should not identify individuals e.g. if a staff survey contained data on an academic staff member in their 20s, this would be a small cohort, and an individual may be identifiable.

8.4 Survey platforms often collect online/device identifiers, but it is possible to turn off at least some of these features. It is unnecessary to collect IP address (which is personal data) and this feature should be turned off. If IP address is collected, the survey is not anonymous. Most SurveyMonkey surveys are sent via 'share a survey link', which records IP addresses of respondents by default. To turn on Anonymous Responses go to the **Collect Responses** section of the survey>click on the name of the collector>click **Anonymous Responses** and choose **On**.

8.5 If a survey is anonymous, it is not possible for respondents to withdraw as it will not be feasible to distinguish their data from that of other respondents.

8.6 Both the survey platform and form used to collect email addresses (see next section) may automatically collect submission time, making it theoretically possible to match an email address with survey responses. In these cases, the survey is not anonymous. Such data matching is not to be done and submission times are to be deleted as soon as possible after survey closure.

9. Incentives for survey participation

9.1 Incentives (such as prizes or vouchers) may be offered on some occasions to encourage participation in a survey. Usually, respondents are invited to enter their email address. This should be collected separately to the answers to survey questions to preserve respondent anonymity.

9.2 It is **not** possible to collect email addresses anonymously within SurveyMonkey. Instead, it is possible to insert a link to a Microsoft Form or web form (latter to be set up by the Digital Communications & Marketing Office) to collect email addresses.

10. Feedback

10.1 Feedback should be given to respondents on surveys they have completed, if feasible. This may not be possible or practical for surveys focused on external respondents, but feedback should normally be provided to current staff and learners. This should include an appropriate level of information e.g. major survey findings, details of actions that will be taken because of survey findings. The feedback mechanism may vary e.g. in-person or shared via email, Moodle or Staff/Student Portal.

11. Survey fatigue

11.1 Learners are heavily surveyed and survey fatigue may negatively impact response rates. Care should be taken to keep surveys interesting, short, relevant and necessary.

11.2 Where it is intended that survey data is used to make important decisions or assessments, including on staff performance, be mindful that low response rates may result in bias or inaccuracies. This should inform how survey data is used.

12. Gender bias

12.1 There is extensive literature on gender bias in teaching evaluations, which may disadvantage female staff. Staff who analyse and report on such surveys should be mindful of this. College surveys should be designed to minimise opportunities for gender bias, and the possibility of unconscious bias should also be borne in mind when analysing survey data.

13. SurveyMonkey account

13.1 Carlow College, St Patrick's has a SurveyMonkey account of which the Digital Communications & Marketing Office is the administrator. 'Teams' may be set up within this account to facilitate the carrying out of surveys by other staff. Each user determines whether a survey that they have created is shared across the Team or not. The norm is that access should be limited to those who require it. Permissions can be edited for existing surveys here: https://help.surveymonkey.com/en/surveymonkey/manage/sharing-surveys/

Appendix 12.1: Survey Approval Application Form

COLÁISTE CHEATHARLACH NAOMH PÁDRAIG
CARLOW COLLEGE ST. PATRICK'S

Survey Approval Application Form

Survey title	
Sponsoring line manager	
Purpose of survey	
Intended respondents	Staff ☐ Learners ☐ Other ☐ (state)
Survey method	SurveyMonkey ☐ Microsoft Forms ☐ Paper survey ☐ Other ☐ (state)
Date survey to be Issued	
Data survey to be closed	
Will aggregate survey data or a report be made available?	Yes ☐ No ☐
To whom will this report be available?	
Will feedback be given to survey respondents?	Yes ☐ No ☐ If no, explain why not:

FOR COMPLETION BY APPROVING FUNCTION

Approval in principle granted	Yes ☐ No ☐
Approval granted by	OOR ☐ HR ☐
Date	

Appendix 12.2: Documentation to be sent to the DPO

COLÁISTE CHEATHARLACH NAOMH PÁDRAIG
CARLOW COLLEGE ST. PATRICK'S

Documentation to be sent to the DPO

1. Survey questions

Insert a hyperlink to survey questions in the column on the right or send them via email to the DPO.**NB:** Questions are to appear exactly as they will to respondents e.g. include provided options and if questions are marked mandatory/optional.	

2. Data Management Plan

Survey title	
Who will have access to raw survey data for the purpose of reviewing it and redacting/deleting inappropriate data?	
Where will raw survey data be stored?	
How will raw survey data be secured?	
How long will raw survey data be kept for?	
Who will analyse survey data?	
How long will reports generated from survey data be kept for?	
Is it intended to match survey data with other data? **NB:** Data matching should not usually occur. It may require a DPIA.	Yes ☐ No ☐ If yes, explain the reason and the other data involved.

3. Data Privacy Information

Insert data privacy information below:

4. Survey Approval Application Form

Insert a hyperlink to the approved Survey Approval Application Form in the column to the right or send it via email to the DPO.	
Has the information recorded in the Survey Approval Application Form changed since it was approved by the relevant College function(s)?	Yes ☐ No ☐ If yes, explain all changes:

FOR COMPLETION BY THE DPO

Documentation agreed	Yes ☐ No ☐
Date	

Appendix 13: Information / Documentation Flows to the DPO

COLÁISTE CHEATHARLACH NAOMH PÁDRAIG
CARLOW COLLEGE ST. PATRICK'S

Information / Documentation Flows to the DPO

This document summarises information and documentation that staff need to supply to the DPO in order to complete various activities covered under the *Data Protection Policy*. Complete information is available in the Policy and its appendices.

Data Subject Request	• Any staff member who receives a data protection request from a data subject should send it to the DPO without delay. Do not reply to it. • A request may be for access to personal data, correction, erasure etc. • See Section 4.4 for further information.
Personal data breach	• A data breach is a security breach involving personal data e.g. unauthorised access, unauthorised disclosure, loss, theft . • Any staff member who is aware of a suspected or actual data breach, or data placed at risk, should contact the DPO without delay. If it is not possible to contact the DPO, contact the President's Office, Director of Strategy and Operations or your line manager in this order. • Further information is available in Section 4.10.
Using new personal data, change of use	• Where it is proposed to use new types of personal data or use existing data for a new purpose, the line manager must notify the DPO in advance. • The line manager may need to update the Records of Processing Activities (Appendix 2). A Data Protection Impact Assessment (DPIA) may be necessary (Appendix 7). • See Sections 4.1 and 4.5 for further information.
Proposed new processor	• Where it is proposed that CCSP uses a new processor (external individual or company that processes data on behalf of CCSP), the line manager must complete the Supplier Assessment Form (Appendix 3) and send it to the DPO.
Proposed new collaboration	• Where CCSP enters into a collaboration with an external partner that involves sharing personal data, a data sharing agreement may be needed. The Collaboration Lead is

	responsible for not fying the DPO at an early stage in discussions, and should use the Assessment Form for Collaborat ons (Appendix 5) to provide relevant informat on to the DPO.
New projects	• If a new project involves personal data use, the Project Lead is to contact the DPO at design stage. An assessment will be carried out by the DPO to determine what act ons are required.
Using personal data under Legit mate Interests	• Where it is proposed to use personal data under the Legit mate Interests basis of the GDPR, the line manager is required to complete a Legit mate Interests Assessment (Appendix 11) and submit it to the DPO.
Conduct ng surveys	• Guidelines on Surveys (Appendix 12) exist for approving any survey carried out by a staf member for work purposes, where the survey will collect personal data. Init ally, HR approves staf surveys in principle, and the Of ce of the Registrar approves learner surveys in principle. Then a data protect on assessment will be conducted. The following draf documentat on should be sent to the DPO once the survey has been approved in principle: survey quest ons, data privacy informat on, and data management plan. • The relevant line manager is responsible for ensuring adherence with the Guidelines.