

Data Protection Policy

Effective from	March 2024	Document number	-
Formal review cycle:	Annual		
Next formal review due	2025-03		
Policy owner:	Vice Principal – Finance & Resources		

Approval required

SMT Y/N	Y	SMT approved/review date	February 2024
Governor Y/N	Y	Audit Committee approved date	7 th March 2024

Publication

Publication							
Website Y/N	Y	Intranet Y/N	Y	Student VLE Y/N		Date published	
Audience		Public, staff, students					
Area/s of Staff Intranet		Policies and Procedures					

Changes made

Version	Author	Date	Section	Changes summary
1.0	G Dixon	Feb 24	All	None – Annual Review

1. Introduction

Craven College is committed to conducting its business in accordance with all applicable UK Data Protection laws and in line with the highest standards of ethical conduct.

This policy written in accordance with Article 24, sets forth the expected behaviours of Craven College Employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a Craven College contact (i.e. the Data Subject) or employee.

Personal data is any information (including opinions and inferences) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. Craven College, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Craven College to complaints, regulatory action, fines and/or reputational damage, and in the case of employees, disciplinary action, and in extreme cases prosecution.

Craven College's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Craven College Employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

This Policy takes account of the legislation provided by the Data Protection Act 2018, and the UK's General Data Protection Regulation (UK GDPR).

2. Key Principles

In accordance with the legislation, Craven College, as a responsible data controller, and registered with the Information Commissioner's Office is required to demonstrate its compliance with the data protection Principles set out in Article 5 of the UK's General Data Protection Regulation and the Data Protection Act 2018.

3. Responsibility

- The College is the official data controller, and if called to account by the Information Commissioner, the Principal would be required to sign any undertaking in response to any enforcement action by the Commissioner.
- The Senior Leadership Team must ensure that all Craven College Employees responsible for the processing of Personal Data are aware of and comply with the contents of this policy.
- The Data Protection Officer (DPO) will provide support and guidance to the College, the Senior Management Team and all staff on data protection compliance.
- The Head of Information Technology is the Senior Information Risk Officer (SIRO) is responsible for the overall risk arising from personal data processing.
- Department managers are appointed Information Asset Owners (IAOs) have local responsibility for data protection compliance.
- All staff are responsible for ensuring compliance.
- All staff are responsible for following the procedures outlines in the policy.

4. Legislation

Data Protection Act 2018
UK General Data Protection Regulation (UK GDPR)
Privacy and Electronic Communications Regulations (PECR)

Data Protection Procedure

Introduction

Craven College is committed to protecting personal data of students, staff and contacts. The procedures set out in the Policy explain how the objectives of the Data Protection Policy will be met and identifies:

1. Key Processes
2. Roles and Responsibilities
3. Objectives
4. Communication
5. Implementation
6. Monitoring
7. Reporting
8. Assessment of Impact
9. Continuous Improvement
10. Associated Documentation

1. Key Processes

This policy applies to all Craven College Departments and staff where a Data Subject's Personal Data is processed:

- In the context of the business activities of the Craven College.
- For the provision or offer of goods or services to individuals (including those provided or offered free-of-charge) by Craven College.
- To actively monitor the behaviour of individuals.

Monitoring the behaviour of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to protect an individual for safeguarding purposes e.g., internet usage, to support the College to:

- i. Taking a decision about them.
- ii. Analysing or predicting their personal preferences, behaviours and attitudes.

This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

2. Roles and Responsibilities

Whilst the College is the official data controller, and if called to account by the Information Commissioner, the Principal would be required to sign any undertaking in response to any

enforcement action by the Commissioner. However, staff at all levels have a responsibility for adherence to data protection principles:

- The Senior Management Team must ensure that all Craven College Employees responsible for the processing of Personal Data are aware of and comply with the contents of this policy.
- The Head of Information Technology is the appointed SIRO (Senior Information Risk Officer) and is responsible for the overall risk arising from the processing of personal data by the College.
- Department Managers are appointed as Information Asset Owners (IAO) and as such are responsible for the processing activities, and data protection compliance within their department. This responsibility is reflected with maintaining the Information Asset Register (IAR) with any changes to, or new processing activities.
- Data Protection Officer (DPO) who operates with independence and is a suitability skilled individual granted all necessary authority. The DPO reports to Craven College's Vice Principal – Finance & Resources who has direct access to the Craven College Board of Governors. The DPO's duties include:
 - i. Informing and advising Craven College and its Employees who carry out Processing pursuant to Data Protection legislation, guidance from the Regulator and best practice;
 - ii. Ensuring the alignment of this policy with UK Data Protection laws. Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
 - iii. Acting as a point of contact for and cooperating with the Information Commissioner's Office (ICO);
 - iv. Determining the need for notifications to the ICO as a result of Craven College's current or intended Personal Data processing activities;
 - v. Making and keeping current notifications to the ICO as a result of Craven College's current or intended Personal Data processing activities;
 - vi. The establishment and operation of a system providing prompt and appropriate responses to Data Subjects wishing to exercise their rights under data protection laws;
 - vii. Informing senior managers, officers, and directors of Craven College of any potential corporate, civil and criminal penalties which may be levied against Craven College and/or its employees for breaches of applicable Data Protection laws.
 - viii. The establishment of procedures and standard contractual provisions relevant to data protection laws to ensure compliance with this Policy by any Third Party which processes Personal Data under a contract with Craven College.
- Craven College Department managers will make sure all Third Parties engaged to process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by Craven College. Any Third-Party processor must be subject to a contract in accordance with Article 28 of the UK GDPR
- All staff are responsible for following the procedures outlines in the policy

If there are any queries in regard to this policy, please consult with the Data Protection Officer for guidance using the following email address: dpo@craven-college.ac.uk.

3. Objectives

The objectives of this policy are:

1. To outline the College's approach to data protection across all levels of the organisation
2. Provide staff, students and third parties with a guide to the College's data protection procedures

4. Communication

The following principles are fundamental to the communication of the Data Protection Policy:

1. The Data Protection Policy will be published on a standardised template
2. The Data Protection Policy will be reviewed by the Vice Principal – Finance & Resources, before being escalated to the SLT for approval.
3. The Data Protection Policy requires ratification by the Audit Committee of the Board.
4. The audience of this policy is all for staff who will be made aware of this via publication on the intranet. Students, partners and members of the public who wish for access the policy may also do so through publication on the website.
5. The document will be published on the intranet and College website.

5. Implementation

The implementation of this policy follows the principles outlined below. Throughout this implementation the definitions used are as outlined in Appendix 1:

- A. Data Protection Principles – All Craven College employees are expected to abide by the College's Data Protection Principles as set out in Appendix 2.
- B. Data Protection by Design - To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

Each Craven College Department must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Vice Principal – Finance and Resources for review and approval. Where applicable, the Information Technology (IT) Department, as part of its IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology on the security of Personal Data. Department managers must ensure they update the Information Asset Register (IAR) to reflect any changes.

- C. Data Collection – Collection of data is subject to the following:

- a) Data Sources - Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation.
- A UK law expressly provides for the collection, Processing or transfer of the Personal Data.

A list of the disclosures that need to be made available to the Data Subject is provided in Appendix 3.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data.
- At the time of first communication if used for communication with the Data Subject.
- At the time of disclosure if disclosed to another recipient following assessment & risk assessment

- b) Data Subject Consent - Craven College will process Personal Data only in accordance with the lawful processing conditions set out in Section 4 below. The Data Protection Officer and other relevant business representatives shall establish a system for obtaining and documenting Data Subject Consent for the collection, processing, and/or transfer of their Personal Data. The system must include provisions for:

- Determining what disclosures should be made.
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

- c) Data Subject Notification - Craven College will provide Data Subjects with information concerning their rights relating to the processing of their Personal Data.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information - The Craven College Department collecting the information, in consultation with the Data Protection Officer, must establish means for documenting the fact that the Data Subject already has the information and how it has been obtained.
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

- d) External Privacy Notices - Each external website provided by Craven College will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law. Refer to Craven College's 'Internet Privacy Notice' and 'Internet Cookie Notice' standard templates for guidance. All Privacy and Cookie Notices must be approved by the Data Protection Officer prior to publication on any Craven College external website.

D. Data Use – The use of data is subject to the following:

- a) Data Processing - Craven College uses the Personal Data of its Contacts for the following broad purposes:
- The general running and business administration of Craven College.
 - To provide services to Craven College customers/students.
 - The ongoing administration and management of customer/student services.
 - To meet its external legal obligations.

The use of a Data Subject's information should always be considered from their perspective and whether the use will be within their rights and reasonable expectations for example, it would clearly be within a Data Subject's reasonable expectations that their details will be used by Craven College to respond to their request for information about the products and services on offer. However, it will not be within their reasonable expectations that Craven College would then provide their details to third parties for marketing purposes (unless they had freely given their informed consent in advance).

Craven College will process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Craven College will not Process Personal Data unless at least one of the following lawful processing conditions is met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the College is subject.
- Processing is necessary for the purposes of a legitimate interest where a Data Subject should reasonably expect their data to be used in a certain way, such as network and information security.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the College.

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

In any circumstance where Consent has not been gained for the specific processing in question, Craven College will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
 - The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the College.
 - The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.
 - The possible consequences of the intended further processing for the Data Subject.
 - The existence of appropriate safeguards pertaining to further processing, which may include Encryption, Anonymisation or Pseudonymisation.
- b) Special Categories of Personal Data - Craven College will only Process Special Categories of Data (also previously known as sensitive personal data) where the Data Subject has explicitly consented to such Processing or where one of the following conditions apply:
- The Processing relates to Personal Data which has already been made public by the Data Subject.
 - The Processing is necessary for the establishment, exercise or defence of legal claims.
 - The Processing is specifically authorised or required by law.
 - The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
 - The Processing is necessary for reasons of substantial public interest on the basis of UK law, which is proportionate to the aims pursued and providing for suitable and specific measures to protect the rights of individuals.
 - The Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health.
 - The Processing is necessary for the purposes of preventive or occupational medicine, for the working capacity of an employee, medical diagnosis, or pursuant to contract with a health professional.

It is unlikely that most of the above conditions would apply in the case of such data that is being processed by the College, except where the individual has given explicit consent. In any situation where Special Categories of Personal Data are to be processed except with the individual's explicit consent, prior approval must be obtained from the Data Protection Officer and the lawful basis for the processing clearly documented and retained.

Where Special Categories of Data are being Processed, Craven College will adopt additional protection measures.

- c) Children's Data - Children (*The age by which an individual is designated a child varies between 13 and 18 in accordance with UK law*) are unable to consent to the Processing of Personal Data for information society services (*Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*). Consent must be sought from the person who holds parental responsibility over the child and Craven College obtains parental consent. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Should any Craven College Department foresee a business need for offering information society services directly to a child, guidance and approval must be obtained from the Data Protection Officer before any processing of a child's Personal Data may commence.

- d) Data Quality - Craven College will adopt all necessary measures to ensure that the Personal Data it processes is complete and accurate in the first instance and is updated to reflect the current situation of the Data Subject.

The measures adopted by Craven College to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification. *Correction may include data erasure and replacement with corrected or supplemented data.*
 - Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
 - The removal of Personal Data if in violation of any of the Data Protection Principles or if the Personal Data is no longer required.
 - Restriction, rather than deletion of Personal Data, insofar as:
 - i. law prohibits erasure.
 - ii. erasure would impair legitimate interests of the Data Subject.
 - iii. the Data Subject disputes that their Personal Data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.
- e) Profiling & Automated Decision-Making - Craven College does not process any data using profiling or automated decision-making.
- f) Digital Marketing - Craven College will not send promotional or direct marketing material to a Craven College Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their informed consent. Any Craven College Department wishing to carry out a digital marketing campaign without obtaining prior consent from the Data Subject must first seek the advice of the Data Protection Officer.

Personal Data Processing for marketing purposes can only be carried out where an individual has 'opted-in' to receive such communications. The Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing-related Processing of their Personal Data must cease

immediately and their details should be kept on a suppression list with a record of their unsubscribe decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of consent to carry out digital marketing to individual business contacts provided that they are given the opportunity to opt-out. This is because business entities are not regarded as 'natural persons'.

- E. Data Retention – To ensure fair Processing, Personal Data will not be retained by Craven College for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

The length of time for which Craven College Departments need to retain Personal Data is set out in the Craven College 'Document Retention Policy'. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

- F. Data Protection - Craven College will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that in the case where Processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that Personal Data is protected against unauthorised destruction or loss (whether deliberate or accidental).
- Ensure that Personal Data collected for different purposes can be and is processed separately.
- Ensure that Personal Data is not kept longer than necessary.

- G. Data Subject Requests - The Data Protection Officer will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, Craven College will consider each such request in accordance with all applicable Data Protection law. No

administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. Appendix B provides a standard form for the collection of information from the Data Subject by the Data Protection Officer to progress the individual's request.

Data Subjects are entitled to obtain, based upon a request made in writing or verbally to the Data Protection Officer and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling.

The right of the Data subject to:

- object to Processing of their Personal Data.
- lodge a complaint with the Data Protection Authority.
- request rectification or erasure of their Personal Data.
- request restriction of Processing of their Personal Data.

All requests received for access to, or rectification of Personal Data must be directed to the Data Protection Officer, who will log each request as it is received. A response to each request will be provided within one month of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised representative. Data Subjects shall have the right to require Craven College to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Craven College cannot respond fully to the request within one month, the Data Protection Officer shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the Craven College individual who the Data Subject should contact for follow up.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that third party data subject's rights.

Craven College reserves the right to deny any requests that are manifestly unfounded.

H. Law Enforcement Requests & Disclosures - In certain circumstances, it is permitted that Personal Data be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If a Craven College Department Processes Personal Data for one of these purposes, then it may apply an exception to the processing rules (with the approval of the Data Protection Officer) outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If Craven College receives a request from a court or any regulatory or law enforcement authority for information relating to a Craven College Contact, you must immediately notify the Data Protection Officer who will provide advice on handling.

I. Data Protection Training - All Craven College employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, each Craven College Department will provide regular Data Protection training and procedural guidance for their staff.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protection Principles set forth in Appendix 2.
- Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms.
- The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person.
- Securely storing manual files, print outs and electronic storage media.
- The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.
- Proper disposal of Personal Data by using secure shredding facilities.
- Any special risks associated with particular departmental activities or duties.

J. Data Transfers - Craven College may transfer Personal Data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection. (for the rights and freedoms of the relevant Data Subjects. Please discuss any proposed transfers to another country outside the EEA, with the College's Data Protection Officer at an early stage). Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism.

Craven College Entities may only transfer Personal Data where one of the transfer scenarios list below applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

Craven College will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where third party Processing takes place, the College will first identify if, under applicable law, the third party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, Craven College will enter into, in cooperation with the Data Protection Officer, an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, Craven College will enter into, in cooperation with the Data Protection Officer, an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Craven College instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches. Craven College has a 'Standard Data Processing Agreement' document that should be used as a baseline template.

When Craven College is outsourcing services to a Third Party (including cloud computing services), they will identify whether the Third Party will process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include, in cooperation with the Data Protection Officer, adequate provisions in the outsourcing agreement for such Processing and Third Country transfers.

The Data Protection Officer shall conduct regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to and monitored by the Craven College Senior Management team.

6. Monitoring

Monitoring of the data protection policy will be carried out through:

1. Compliance Monitoring - To confirm that an adequate level of compliance is being achieved by all Craven College Departments in relation to this policy, the Data Protection Officer will carry out an annual Data Protection compliance audit for all such Departments. Each audit will, as a minimum, assess:
 - a. Compliance with Policy in relation to the protection of Personal Data, including:
 - b. The assignment of responsibilities.

- c. Raising awareness.
 - d. Training of Employees.
2. Complaints Handling - Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Officer, then the Data Subject may, at their option, will be advised of their right to complain to the Information Commissioner.

7. Reporting

Reporting of data protection will be subject to:

- 1. Mandatory Training completion of annual data protection training for all staff.
- 2. Breach Reporting - Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can be made via e-mail at dpo@craven-college.ac.uk or by calling the Data Protection Officer on 01756 791411.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, the Craven College SMT will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response and the inform the Chair of the Board, where appropriate.

8. Assessment of Impact

The impact of this policy has been assessed and reviewed alongside other data protection considerations within the College. As data protection is a fundamental requirement for the College the impact of this is wide ranging and any breaches could have significantly operational, financial and reputational impacts. As such the annual training and awareness amongst the whole staff is a key requirement to adherence with this policy.

9. Continuous Improvement

Continuous improvement in this policy will be achieved through:

- 1. Regular dialogue with a qualified DPO to highlight any changes in legislation that need to be adopted
- 2. Regular review of data breaches to ensure lessons are learnt and procedures implemented to prevent future occurrences
- 3. Annual review of the data protection policy for completeness and accuracy
- 4. Annual mandatory training requirement for all staff on data protection and related matters.

10. Associated Documentation

Listed below are documents that relate to and are referenced by this policy.

1. Internet / Intranet Privacy Notice template
2. CCTV Privacy Notice
3. Internet Cookie Notice template
4. Information Security Policy
5. Data Subject Request Handling Procedure
6. Personal Data Retention Schedule
7. Standard Data Processing Agreement
8. Standard Provisions for Outsourcing Agreement
9. Breach Policy
10. Document Retention Policy

Appendix 1 – Definitions

Employee	An individual who works part-time or full-time for Craven College under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees.
Third Party (including a data processor – see below)	An external organisation with which Craven College conducts business and is also authorised to, under the direct authority of Craven College, Process the Personal Data of Craven College Contacts and employees.
Personal Data	Means any information relating to a natural person – a data subject - who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Contact	Any past, current or prospective Craven College customer including students, parents and businesses.
Identifiable Natural Person	A living person or data subject (but this does not include legal undertakings, legal persons or business entities). Note that the normal rules of confidentiality still apply to information relating to deceased persons.
Data Controller	A natural or legal person, public authority, agency or other body or organisation which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
Craven College Department	A Craven College area run by a designated manager. Such areas will normally, but not always, hold a designated budget.
Data Protection Officer (DPO)	A Data Protection Officer (DPO) is a role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements
Data Subject	The identified or Identifiable Natural Person to which the data refers.
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Protection Authority	An independent public authority responsible for regulating the application of the relevant Data Protection regulation set forth in UK law (in the UK this refers to the Information Commissioner).
Data Processors	A natural or legal person, or body which processes Personal Data on behalf of a Data Controller.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health, or sex life and sexual orientation; and genetic data or biometric data for the purpose of uniquely identifying a natural person.
Third Country	Any country which may not be recognised as having an adequate level of legal protection for the rights and freedoms of data subjects in relation to the processing of Personal Data.
Profiling	Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable natural person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Binding Corporate Rules	The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Personal Data Breach	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.
Encryption	The process of converting information or data into code, to prevent unauthorised access. The minimum standard is FIPS 140-2 and FIPS 197.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Appendix 2 – Craven College Data Protection Principles

Principle 1: Fairly and Lawfully and in a transparent manner

Personal data shall be processed fairly and lawfully. This means that Craven College must have:

- legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means Craven College must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Adequate, relevant and minimised

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means Craven College must not collect or store any Personal Data beyond what is strictly required.

Principle 4: Accuracy

Personal Data shall be accurate and, kept up to date. This means Craven College must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means Craven College must, keep or store Personal Data for no longer than is necessary consistent with the original processing purpose.

Principle 6: Security and Confidentiality

Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. Craven College must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times. This includes technical as well as organisational means of protecting data, including the awareness of staff.

Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means Craven College must demonstrate to the satisfaction of the ICO that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Appendix 3 - Information Notification to Data Subjects

The table below outlines the various information elements that must be provided by the Data Controller to the Data Subject depending upon whether or not Consent has not been obtained from the Data Subject.

Information Requiring Notification	With Consent	Without Consent
The identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative.		✓
The original source of the Personal Data, and if applicable, whether it came from a publicly accessible source.		✓
The contact details of the Data Protection Officer, where applicable.		✓
The purpose(s) and legal basis for Processing the Personal Data.		✓
The categories of Personal Data concerned.		✓
The recipients or categories of recipients of the Personal Data.	✓	✓
Where the Data Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data was originally collected, the Data Controller shall provide the Data Subject, prior to that further Processing, with information on that other purpose.	✓	✓
Where the Data Controller intends to transfer Personal Data to a recipient in a Third Country, notification of that intention and details regarding adequacy decisions taken in relation to the Third Country must be provided.	✓	✓
The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.		✓
Where applicable, the legitimate interests pursued by the Data Controller or by a Third Party.		✓
The existence of automated decision-making (including Profiling) along with meaningful information about the logic involved and the significance of any envisaged consequences of such processing for the Data Subject.	✓	✓