

FORCE

42000

50000

37500

36000

37500

ONE: A

01 2152 1233 1234
02 1234 1234 1235
03 1234 1234 1235
04 1234 1234 1235
05 1234 1234 1235

Quality Assurance Handbook

SETANTA COLLEGE

Section 9: Information and Data Management



SETANTA
College

9.1 Policy on Information Management

9.1.1 Definition

Information management can be defined as "recorded information, in any form, created or received and maintained by the College or person in the transaction of business or conduct of affairs and kept as evidence of such activity". Records occur in all types of recording media.

9.1.2 Purpose

The College recognises that the efficient management of its records is necessary in order to support its core functions, to comply with its legal and regulatory obligations and to enable the effective management and operation of the College. It is committed, through the Information Management Policy, to creating, keeping and maintaining those records which document its principal activities, including teaching, research, the administration of its resources and the protection of the rights and interests of the College and its stakeholders.

9.1.3 Scope

This policy applies to all Setanta College staff, Learners and alumni and to all College records and information, including but not limited to:

- Setanta College Learner Data
- Setanta College Staff Data
- Setanta College Financial Data
- Setanta College Commercial Data
- Setanta College Intellectual Property
- Setanta College Academic Data.

9.1.4 Policy Statement

Setanta College will develop internal and public information systems that allow for the collection, processing, and use of information by staff so as to ensure the effective support and development of academic programmes and associated activities.

9.1.5 Information Management mechanisms

i. College Information Systems

Setanta College provides information on its courses through the college website. Information provided outlines the following:

- Titles of each programme offered by Setanta College
- Information about the relevant awarding body
- If applicable the relevant level of qualification on the National Framework of Qualifications
- Information on entry requirements, progression and transfer for each programme
- Details for procedures for Protection of Enrolled Learners

- Details of fees and methods of payment, and refunds
- Details on Quality Assurance for Transnational and Collaborative programmes where applicable
- Details of component modules, programme duration, and assessment methodologies, and the target market
- Where a programme has recognition or accreditation from a professional body or is delivered in partnership with another institution this information is also included.
- Details of English Language requirements for applicants whose first language is not English
- Contact details for further queries relating to details of the programme

All information is compiled by the College Registrar and approved by the Senior Management Team prior to release and is in line with QQI guidelines and relevant legislation. Where information or logos of a professional body are being utilised within the literature or website, approval is sought from that third party in advance.

ii. Learner Information Systems

Setanta College ensures that it keeps up to date Learner information. This data includes personal details, contact information, continual assessment results, stages completed, subject choices and results, awards conferred and classification.

The database system is robust and comprehensive, capable of:

- Maintaining secure Learner records for current use and historical review
- Providing reports required for internal quality management
- Generating data required for and compatible with QQI's systems
- Generating statistical and other reports to meet QQI information requirements

The College has the required technical expertise for the ongoing operation of information systems and has arrangements in place for back-ups of all data in the case of technical failure.

Obligations under GDPR data protection legislation are complied with. This includes establishing data access controls, data backup systems and Learner information material making clear what personal data will be required to be collected and for what purpose.

Administrative and information technology resources should be sufficient to ensure that the database is maintained securely and that data, particularly that relating to Learner assessment are accurate and complete.

iii. Management Information Systems

The College management information system enables necessary information to be stored and channelled to where it is needed when it is needed. It facilitates timely and accurate analysis and research by Setanta College on performance indicators and College objectives.

In particular information regarding Learner admissions, progression, Learner result and Learner retention are generated and used in the appropriate monitoring and review processes.

The information system also collects and makes available to QQI information relating to completion rates in accordance with the [QQI Monitoring Policy 2014](#)

9.1.6 Responsibility for this Policy

The College Registrar assumes the role of the Data Protection Controller. In addition, all employees who create and keep records as part of their official duties are responsible for them in a wide sense. An external provider supports and maintains/back-ups on the online learning portal in conjunction with the IT Manager and College Registrar. The Student services manager is responsible for the secure transferring of Learner Data to third party accrediting bodies such as QQI. The Senior Management Team is responsible for the templates used for management reports.

9.1.7 Policy Control Sheet

Policy Area	Information and Data Management
Policy Title	Information Management
Approval Date	3/9/2019
Effective Date	3/9/2019
Review Date	1/9/2020
Relevant Supporting Policies	<ul style="list-style-type: none">- Core Statutory Quality Assurance Guidelines (2016), QQI- Qualification and Quality Assurance (Education and Training) Act 2012- 2012; European Standards and Guidelines for QA in the European Higher Education Area, QQI Core Quality Assurance Guidelines- QQI Monitoring Policy 2014- General Data Protection Regulations (GDPR)
Monitoring Procedures	<ul style="list-style-type: none">- Management reporting templates- Senior Management Team: Review of any error reporting or data breaches

9.2 Data Protection Policy

9.2.1 Definition

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

i. Personal Data

Any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to an individual.

ii. Special Categories of Personal Data

A category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation. The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

iii. Data Controller

Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

iv. Data Subject

A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

v. Data Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

vi. Data Protection Contact

A person appointed by Setanta College to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members, Learners, and all data subjects or potential data subjects. The appointed individual at the College is the College Registrar.

vii. Relevant Filing System

Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

viii. 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.

ix. Supervisory Authority

An independent public authority which is established by a Member State pursuant to Article 51; In Ireland, the supervisory authority is the Data Protection Commissioner.

9.2.2 Purpose

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Setanta College. This includes obligations in dealing with personal data, to ensure that the organisation complies with the requirements of the EU General Data Protection Regulation (GDPR).

9.2.3 Scope

The policy covers both personal and special categories of personal data (sensitive data) processed in relation to data subjects by Setanta College. The policy applies equally to personal data held in manual and automated form. All Personal and Special Categories of Personal Data will be treated with equal care by Setanta College. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

9.2.4 Policy Statement

Setanta College is committed to complying with the Data Protection principles set out in the GDPR. This Policy applies to all Personal Data collected, processed and stored by Setanta College in relation to its staff, Learners, and service providers. Setanta College makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

9.2.5 Procedures for this Policy

i. Procedure for Enrolled Learners

Learners read and agree to the Learner Data Protection notice which is provided as a resource on the college website prior to enrolling onto a programme of study.

ii. Setanta College as a Data Controller

During its daily organisational activities, Setanta College acquires, processes and stores personal data in relation to:

- Employees
- Former employees
- Learners
- Applicants (to programmes and employment vacancies)
- Graduates
- Third party service providers engaged by the College

In accordance with the GDPR, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, Setanta College is committed to ensuring that its staff have enough awareness of the GDPR in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Contact is informed, without delay, in order that appropriate corrective action is taken.

As a higher education provider, there is regular and active exchange of personal data between Setanta College and its Data Subjects. In addition, Setanta College may exchange personal data with Data Processors and or Joint Data Controllers on the Data Subjects' behalf. This is consistent with Setanta College's obligations under the terms of its contract with its Data Processors, Joint Data Controllers and its Data Subjects. This policy provides the guidelines for this exchange of information, as well as the procedure to follow if a Setanta College staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the College Registrar, as the Data Protection Contact, to seek clarification.

iii. Data Protection Contact

All personal data enquiries, or requests to exercise an individual's rights as a data subject, can be directed to The College Registrar, Setanta College, Thurles Chamber Enterprise Centre, Nenagh Road, Thurles, Co. Tipperary or by email to admin@setantacollege.com. If an individual is dissatisfied with the information provided or believe the request to exercise their rights has not been addressed, the individual concerned can make a complaint to the supervisory authority. As Setanta College operates primarily in Ireland, the supervisory authority is the Data Protection Commissioner who can be contacted through the following means:

By post: Office of the Data Protection Commissioner, Canal House, Station Road, Port Arlington, Co. Laois, R32 AP23, Ireland.

By phone: +353 (0761) 104800 | **By email:** email info@dataprotection.ie

iv. Data Subjects' Rights

Under GDPR data subjects have increased rights and data controllers are required to notify data subjects of their rights. Individuals have the right to:

- Be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- Withdraw consent, where consent is the legal basis for data processing
- Access their personal data (a data subject access request).
- Have inaccurate personal data rectified or completed if incomplete.
- Have personal data erased (the right to be forgotten) in certain circumstances
- Request the restriction or suppression of their personal data, in certain circumstances
- Data portability, allowing individuals to reuse their data across different services, where feasible
- Object to personal data processing, in certain circumstances

To exercise any of these rights, please use the data protection contact details provided in this Policy. Where we require additional information from you to verify your identity and the legitimacy of the request or to establish the specific reasons for the request to enable Setanta College to respond appropriately we will do so in a timely manner. There is normally no fee applied in respect of any rights

v. Third-Party processors

During its role as Data Controller, Setanta College may engage several Data Processors to process Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the GDPR.

Setanta College recognises that it remains the Data Controller and the College is thus responsible for how the data is used.

vi. Joint Data Controllers

In certain circumstances, in its role as Data Controller, Setanta College may be the joint controller for personal data of data subjects. In each case, each party recognises the full extent of the Data Controller obligations in relation to the Personal Data, the specific purpose or purposes for which it is collected, processed, retained and transmitted and the requirement to process the data in compliance with the GDPR.

Irrespective of whether Setanta College acts as sole data controller or as joint data controller, data subjects may exercise their rights under GDPR in respect of Setanta College's data controller obligations. Any joint controller must extend the same rights to the data subjects. In such cases, neither Controller is responsible for the data processing determining by the joint controller.

In addition to cases where the College is required or permitted by law to disclose your personal data to others, the College may disclose your personal data in connection with the purposes referred to above. These include, but are not limited to:

- Quality Qualifications Ireland
- Higher Education Colleges Association and the HECA PEL Committee
- Funding bodies, research sponsors, industry funders and other agencies that support, sponsor or otherwise have a valid interest in your education
- The Higher Education Authority (HEA) (see the HEA's Learner Data Collection Notice http://hea.ie/about-us/data_protection/)
- National Forum for teaching and learning
- Providers of academic and other services to the College (who are obliged to keep your data safe and secure), which may also include, but is not limited to, wholly/majority owned subsidiaries of the College
- Examination Boards and External Examiners
- Government departments where required (e.g. Department of Education and Skills, Department of Employment Affairs and Social Protection, Revenue)
- Potential employers (where you have requested us to provide a reference)
- The College's insurance brokers and providers where required for administering claims
- Professional and regulatory bodies where programmes are accredited by such bodies
- External auditors
- Other higher education institutions, partners or research organisations to or from which a Learner transfers or pursues an exchange programme or where a Learner's programme is being run collaboratively
- Plagiarism detection service providers (e.g. Turnitin) to ensure academic standards.

9.2.6 Data Protection Principles

The following key principles are enshrined in the GDPR and are fundamental to the Setanta College Data Protection policy. In its capacity as Data Controller, Setanta College ensures that all data shall be:

- a) Processed lawfully, fairly and in a transparent manner in relation to individuals. Setanta College will meet this obligation in the following way:
 - Setanta College will ensure that collection of the data is justified under one of the lawful processing conditions – legal obligation, contractual necessity, etc.
 - Where required and no alternative appropriate legal basis for processing is identified, the informed consent of the Data Subject will be sought before their data is processed.
 - The data subject will be fully informed about the consent requested and the right to withdraw consent
 - Where Setanta College intends to record activity on CCTV or video, this will be brought to the attention of data subjects and an appropriate policy will be made publicly available.

- Processing of the personal data will be carried out only as part of Setanta College's lawful activities, and Setanta College will safeguard the rights and freedoms of the Data Subject
 - The Data Subject's data will not be disclosed to a third party other than to a party contracted to Setanta College and operating on its behalf, or in cases where there is a legal obligation, or it is in the vital interests of the data subject (or other parties), or in the national interest
- b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. Setanta College will fulfil its obligation in this regard by:
- Only obtaining data for purposes which are specific, lawful and clearly stated.
 - Affording the Data Subject, the right to question the purpose(s) for which Setanta College holds their data,
 - Ensuring Setanta College can clearly state the purpose or purposes for data processing.
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Setanta College will fulfil its obligation in this regard by ensuring use of the data by Setanta College will be compatible with the purposes for which the data was acquired.
- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Setanta College will fulfil its obligations in this regard by:
 - Ensuring that appropriate mechanisms (audits, administrative and IT validation processes) are in place to conduct regular assessments of data accuracy;
 - Conducting periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date.
 - Providing means for data subjects to verify the accuracy, currency and completeness of their personal data and opportunity for correction or completion to be implemented, as required.
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals. Setanta College will fulfil its obligations in this regard by:
- Developing, publishing and implementing a records retention policy which clearly outlines the retention periods for personal data based upon the purpose for which the data was collected and the legal basis upon which retention is determined.

- Implementing regular audits to ensure the full and proper adherence to the records retention policy
 - Training staff in their responsibilities and obligations regarding retention of personal data
 - Implementing appropriate measures for the secure destruction, deletion or archiving of personal data at the end of the retention period.
- f) 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, using appropriate technical or organisational measures. Setanta College will fulfil its obligations in this regard by:
- Employing appropriate standards of security in order to protect the personal data under its care.
 - Implementing security measures to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Setanta College in its capacity as Data Controller.
 - Limiting access to and management of staff and Learner / graduate records to those staff members who have appropriate authorisation and password access.
 - Providing appropriate training for staff to know their obligations and responsibilities in respect of personal data.
 - Implementing appropriate measures to determine security of data transfers to other countries and only transferring outside of the EU where the transfer is:
 - made with the individual's informed consent
 - necessary for the performance of a contract between the individual and organisation or for pre-contractual steps taken at the individual's request;
 - necessary for the performance of a contract made in the interests of the individual between the controller and another person;
 - necessary for important reasons of public interest;
 - necessary for the establishment, exercise or defence of legal claims;
 - necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
 - made from a register which under Irish or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

9.2.7 Data Subject Access Requests

As part of the day-to-day operation of the organisation, Setanta College staff engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by Setanta College, such a request gives rise to access rights in favour of the Data Subject. Please view Setanta College 9.3 Data Access Request Policy

9.2.8 Personal Data Security Breaches

Setanta College is obliged under the Data Protection Acts, 2018 and any subsequent legislation to keep personal data safe and secure and to respond promptly and appropriately

to data security breaches (including reporting such breaches to the Data Protection Commissioner in certain cases).

It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the College.

9.2.9 Implementation

As a Data Controller, Setanta College ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage Setanta College’s data in a compliant manner will be viewed as a breach of contract and may be pursued through the courts.

Failure of Setanta College to process Personal Data in compliance with this policy may result in disciplinary proceedings.

9.2.10 Responsibility for this Policy

The Data Controller (College Registrar) is responsible for implementing this policy. The controller has a wide range of responsibilities under the GDPR and national Data Protection legislation. All employees who process personal data are required to abide by this Policy and Associated Documentation, both now existing and introduced in the future. If all employees are not compliant with this policy they can be subject to disciplinary proceedings.

9.2.11 Policy Control Sheet

Policy Area	Information and Data Management
Policy Title	Data Protection Policy
Approval Date	3/9/2019
Effective Date	3/9/2019
Review Date	1/9/2020
Relevant Supporting Policies	<ul style="list-style-type: none"> - Qualifications and Quality Assurance (Education and Training) Act 2012. - Core Statutory Quality Assurance Guidelines (2016), QQI. - Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG), 2015. - General Data Protection Regulation (GDPR), 2016 - Data Protection Act 2018
Monitoring Procedures	<ul style="list-style-type: none"> - Induction surveys - Learner feedback - Tutor feedback - College Registrar Report to Senior Management Team

9.3 Data Access Request Policy

9.3.1 Definitions within this Policy

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this policy.

i. Personal Data

Any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a individual.

ii. Special Categories of Personal Data

A category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation.

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

iii. Data Controller

Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

iv. Data Subject

A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

v. Data Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

vi. Data Protection Contact

A person appointed by Setanta College to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members, Learners, and all data subjects or potential data subjects. The College Registrar acts as the Data Protection Contact.

vii. Relevant Filing System

Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

viii. 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.

ix. Supervisory Authority

An independent public authority which is established by a Member State pursuant to Article 51; In Ireland, the supervisory authority is the Data Protection Commissioner.

9.3.2 Scope

Any personal data processed by Setanta College is within the scope of this policy. Individuals have the right to obtain the following:

- Confirmation that Setanta College is processing their personal data;
- A copy of their personal data; and
- Other supplementary information

9.3.3 Purpose

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information in accordance with the [Data Protection Act 2018](#). It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

9.3.4 Data Access Request Policy

The following processes regarding data access request are applied at the College.

- i. An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). For this reason Setanta College will take reasonable steps to verify that the information requested falls within the definition of personal data. Individuals can make a subject access request through the Data Protection Controller – admin@setantacollege.com, using the official Data Access Request form. Setanta

College encourages the submission of requests in writing, to ensure it is wholly understood what is being requested at what specific time and date.

- ii. A record of all subject access requests received will be retained. GDPR places a responsibility on Data Processors to respond to a subject access request within one month, in most circumstances. For implementation of this policy Setanta College interprets that to be 30 calendar days. An extension of the response time by a further two months is acceptable if the request is complex or Setanta College have received several requests from the individual. In such cases Setanta College will notify the individual within one month of receiving their request and explain why the extension is necessary.
- i. There may be circumstances when Setanta College needs to verify the identity of the individual making the access request. In such case, proof of identity will be sought as soon as possible, before responding to the request. The period for responding to the request will commence once the proof of identity has been received. In certain case an access request may be made by a third party such a solicitor or representative. This is permissible where the third party can provide verifiable evidence which confirms their authority to do so.
- ii. Subject access requests are to be processed free of charge in most circumstances. Where the request is manifestly unfounded or excessive Setanta College may charge a reasonable fee for the administrative costs of complying with the request. A reasonable fee may also be charged if an individual requests further copies of their data following a request. This fee will be based on the administrative costs of providing further copies. Unless specifically requested otherwise, Setanta College will normally respond to a subject access request through a commonly used electronic format. In certain circumstances a data subject may be invited to view their data on Setanta College premises where it is not feasible or practicable to provide another means of access. Responding to a subject access request should not adversely affect the rights and freedoms of others – including the right to privacy, trade secrets or intellectual property.
- iii. Where the information sought includes the personal data of others Setanta College is not obliged to comply with the request except if:
 - The other individual has consented to the disclosure; or
 - It is reasonable to comply with the request without that individual's consent.
- iv. In determining whether it is reasonable to disclose the information, Setanta College will consider all relevant circumstances, including:
 - The type of information that would be disclosed
 - Any duty of confidentiality to the other individual
 - Any steps taken to seek consent from the other individual
 - Whether the other individual can give consent and any express refusal of consent by the other individual

- v. A subject access request will also include the provision of personal data held by any processor operating on behalf of Setanta College. It does not include data held by a joint controller. In such circumstances a separate access request should be made to the joint controller. Setanta College views an access request as relating to the data held at the time the request was received. However, in some instances, routine use of the data may result in it being amended or deleted while the access request is being processed. In such cases Setanta College will supply information it holds at the time of responding to the request. This does not permit Setanta College to delete or amend data specifically because of an access request.
- vi. Setanta College will seek to provide information to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It is noted that there is no obligation to interpret, type or re-write poorly handwritten notes or translate information into a language other than English. Setanta College reserves the right to process an access request where it is manifestly unfounded or excessive, considering whether the request is repetitive in nature. In such cases justification for the decision will be provided in writing, within one month.
- vii. The data subject will be advised of their right to make a complaint or to seek judicial remedy. Further details on the rights of the Data Subject are available on the Data Protection Commissioner's website www.dataprotection.ie or through contacting the Data Protection Commissioner

By post: Office of the Data Protection Commissioner, Canal House, Station Road, Portarlinton, Co. Laois, R32 AP23, Ireland.

By phone: +353 (0761) 104800, or

By email: email info@dataprotection.ie

9.3.5 Procedures related to the Data Access Request Policy

- i. Where an individual exercises their right to access personal data, a data subject should submit their request in writing using the official Setanta College Personal Data Access Request Form to the Setanta College Data Protection Contact, by email to admin@setantacollege.com where it will be recorded, and the date of receipt noted. Where a request is received through other means or through an alternative member of Setanta staff, the date of first receipt will also be recorded. Staff members receiving a request to access personal data must forward it to the Data Protection Contact as an urgent priority. In the case of absence of the Data Protection Contact, the matter should be forwarded to the College Registrar. To assist in providing a full response, the data subject is requested to be as specific as possible about the information they wish to see and provide as much information as possible to assist in locating it.

- ii. Setanta College may hold a substantial amount of data across different departments, but an individual may only want access to a small portion of that data. Setanta College therefore requests individuals to be as specific as possible about the information they wish to see. An individual seeking amendment to their personal data processed by Setanta College, must specify what data is incorrect and provide the correct version of same.
- iii. Evidence to support the required change of personal information may be required in some cases, e.g. change of name. We will advise you if this arises. Upon receipt of an access request, the Data Protection Contact will determine whether further information, including proof of identity or authority, is required. Once the Data Protection Contact is satisfied all information required is available the data access request will be processed. Where this requires assistance from other individuals they will be notified of the information request and the timeframe in which they must provide it.
- iv. The Data Protection Contact will compile the response to the data access request, including the provision of supplementary information. The response will be issued to the data subject, normally in electronic format, except where specified otherwise or where this is not feasible and practicable. A copy of the response will be retained by the College for a period of 12 months. The data subject will be notified of their right to correction, right to erasure, right to withdraw consent and right to complain to the supervisory authority (Data Protection Commissioner).

9.3.6 Implementation of the Data Access Request Policy

As a Data Controller, Setanta College ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage Setanta College's data in a compliant manner will be viewed as a breach of contract and may be pursued through the courts. Failure of Setanta College to process Personal Data in compliance with this policy may result in disciplinary proceedings.

9.3.7 Policy Control Sheet

Policy Area	Information and Data Management
Policy Title	Data Access Request
Approval Date	3/9/2019
Effective Date	3/9/2019
Review Date	1/9/2020
Relevant Supporting Policies	<ul style="list-style-type: none"> - Core Statutory Quality Assurance Guidelines (2016), QQI - Qualification and Quality Assurance (Education and Training) Act 2012 - 2012; European Standards and Guidelines for QA in the European Higher Education Area, QQI Core Quality Assurance Guidelines - General Data Protection Regulations (GDPR) – 2016 - Data Protection Act 2018
Monitoring Procedures	<ul style="list-style-type: none"> - Teaching Staff Appraisals - Annual Staff Survey - College Registrar Report to Senior Management Team - Academic Council Annual Report