INFORMATION SECURITY POLICY

Document Title	**Information Security Policy (formerly Data Protection)**
Version	**1.0**
Approved by	**Executive Director of Finance and Resources**
Date approved	**25 Jan 2021**
Effective date	**25 Jan 2021**
Date of next review	**26 Jan 2023**
Lead responsibility	**Technology and Innovation Manager**

1. Introduction

1.1. Information (Data) is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as Derwentside College, where information will relate to learning and teaching, administration and management. The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of Derwentside College. Any failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for Derwentside College to recover.

1.2. This policy is concerned with management and security of the College's information assets (an information asset is defined to be an item or body of information, an information storage system or and information processing system which is of value to the College. It is not restricted to digital information assets). It will provide the guiding principles and responsibilities necessary to safeguard the security of the College's security systems. Supporting policies, codes of practice, procedures and guidelines will provide further details.

1.3. The principles defined in this policy will be applied to all of the physical and digital information assets for which Derwentside College is responsible irrespective of storage location.

2. Purpose

2.1. The purpose of this policy is to provide a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur. In particular,

- Ensure the protection of all Derwentside College information systems (including but not limited to all computers, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
- Make certain that all users are aware of and comply with all current and relevant UK and EU legislation.
- Provide a safe and secure information systems working environment for staff, students and any other authorised users.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the information that they handle.
- Protect Derwentside College from liability or damage through the misuse of ICT facilities.
- Respond to feedback and update as appropriate.

3. Scope

3.1. This policy provides a framework for the management of information security throughout the College. It applies to:

- All those with access to Derwentside College information systems, including staff, students, visitors, partners and contractors.
- Any systems attached to the College computer or telephone networks and any systems provided or managed by the College.
- Mobile devices used to connect to the College networks or hold College information.
- All information processed by the College pursuant to its operation activities, regardless of whether it is processed digitally or in paper (hard copy) form.
- Any communication sent to or from the College and any information held on systems external to the College's network.
- All external parties that provide services to the College in respect of information processing facilities and business activities.
- Principal information assets including the physical locations from which the College operates.

4. Policy / Principles

4.1. The College needs to keep certain information (data) about its employees, students and other users to allow us to monitor recruitment, attendance, performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998 and in the General Data Protection Regulation 2018 (GDPR). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside of the European Economic Area, unless that country has equivalent levels of protection for personal data.

4.2. The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times.

4.3. Responsibilities of Staff

Information about yourself

4.3.1. All staff are responsible for:

- Checking that any information they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information, which they have provided, i.e. change of address.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless they have been reported.

Information about other people

4.3.2. All staff must comply with the following guidelines:

4.3.3. Data about individuals will be processed on a regular basis, when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure through the enrolment process, that all users give their consent to this type of processing, as required by the 1998 Act and GDPR 2018 The information that staff deal with on a day to day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address.
- Details about attendance, course work marks and grades and associated comments.
- Notes of personal supervision, including matters about behaviour and discipline.

4.3.4. Information about an individual's physical or mental health; sexual orientation; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with consent.

All staff have a duty to make sure that records are:

- Accurate;
- Up-to-date;
- Fair;
- Kept and disposed of safely, and in accordance with College policy.

4.3.5. The College will designate staff in the relevant area as "authorised staff". These staff are the only staff authorised to access data that is:

- Not standard data; or
- Sensitive data

4.3.6. The only exception to this will be if a non-authorised member is satisfied and can demonstrate that processing of the data is necessary:

- In the best interests of the individual or staff member, or a third person, or the College AND
- He or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.
- This should only happen in very limited circumstances. E.g. an individual is injured and unconscious and in need of medical attention, or a member of staff tells the hospital that the individual is pregnant or a Jehovah's Witness.

4.3.7. Authorised staff will be responsible for ensuring that all personal data is kept securely. In particular staff must ensure that personal data is:

- Put away in lockable storage
- Not left on unattended desks or tables (clean desk)
- Unattended ICT equipment should not be accessible to other users (logout or lock PC)
- ICT equipment used offsite must be encrypted and password protected.
- Data files on removable media (CD, USB drives, email attachments) must be encrypted and password protected.
- Paper records containing personal data must be securely shredded where appropriate.

4.3.8. Staff must not disclose personal data to any individual, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the Information Security Policy.

4.3.9. Staff shall not disclose personal data to any other member of staff except with the authorisation or agreement of the designated data controller, or in line with the College Information Security Policy.

4.3.10. Before processing any personal data, all staff should consider the following.

- Do you really need to record the information?
- Is the information "sensitive"?
- If it is sensitive, do you have the data subject's express consent?
- Has the individual been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the individual or the safety of others to collect and retain the data?

4.4. Rights to Access of Information

4.4.1. Staff, individuals and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the College Standard Request Form for Access to Data and send it to their Line Manager or Customer Services.

4.4.2. The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days (in line with legislation) unless there is a good reason for the delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

4.5. Subject Consent

4.5.1. In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the College processing some specified classes or personal data is a condition of acceptance of an individual onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

4.5.2. Some jobs will bring the applicants in contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactment to ensure that staff are suitable for any job offered. The College also has a duty of care to all staff and learners and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

4.5.3. The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

4.5.4. Therefore, all prospective staff and learners will be asked to sign either an appropriate HR form or an individual document regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such documents may result in the offer being withdrawn.

4.6. The Data Controller and the Designated Data Controller(s)

4.6.1. The College as a corporate body is the data controller under the Act, and the board is ultimately responsible for implementation. However, the designated data controllers will deal with day to day matters.

4.6.2. The nominated Data Protection Coordinator is the Director of Finance and Resource whose contact details can be found on the College's StaffNet. In the event of the Director of Finance and Resource being unavailable, the nominated deputy for the Data Protection Coordinator is a member of the SMT.

4.6.3. The College's designated data controllers are the Director of Finance and Resource who is responsible for all data relating to staff and finance and the MIS Manager who is responsible for all data relating to learners

4.7. Retention of Data

Please see Appendix 1 for the guidelines for the retention of personal data.

5. Relevant Legislation / Regulation

5.1. The following legislation and regulations apply to this policy / procedure:

- The Computer Misuse Act 1990
- Data Protection Act 1998
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Defamation Act 1996
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Criminal Justice and Immigration Act 2008
- Terrorism Act 2008
- Counter-Terrorism and Security Act 2015 (Prevent)
- General Data Protection Regulation 2018

6. Related Documents

6.1. The following related documents are relevant to this policy / procedure:

- Antivirus Policy
- Backup Policy
- Email Usage Policy
- Network Account Policy
- Acceptable Usage Policy
- Password Policy
- Physical Security Policy
- Remote Access Policy
- System Update Policy
- Encryption Policy

7. Accountability

7.1. The Technology and Innovation Manager is responsible for the drafting and implementation of this policy.

7.2. He or she is also responsible for ensuring that this document is regularly reviewed and updated – and is the first contact point for managers seeking advice and guidance about the Information Security Policy or making enquiries about its interpretation.

7.3. All managers are responsible for ensuring that they and their team members follow the requirements set out in this document.

7.4. All employees are responsible for adhering to the requirements set out in this document.

8. Equality & Diversity

8.1. The College has paid due regard to equality considerations during the preparation and implementation of this Policy and Procedure.

8.2. These considerations included the potential for any differential negative effect on the grounds of age, disability, gender reassignment, pregnancy and maternity, race (including ethnic or national origins, colour or nationality), religion or belief (including lack of belief), sex, sexual orientation, marriage or civil partnership.

8.3. The College's judgement is that there is no such negative effect on those grounds and, consequently, no potential breach of the Equality Act 2010.

8.4. The operation of this Policy and Procedure will be monitored by the Personnel Manager in order to establish that no unlawful discrimination is taking place and to identify opportunities for the College to enhance equality of opportunity and fair treatment.

9. Review

9.1. This document will be reviewed by January 2023.

9.2. The Technology and Innovation Manager will undertake this review, taking into account the outcomes of the monitoring process, legislative changes and developments in good practice.

9.3. As part of the review, the Technology and Innovation Manager will seek and consider the views of the College's employees and of the recognised trade unions.

9.4. The outcome of the review will be reported to the Senior Management Team.

10. Document Identification

Category [select ONE only]	☐Programmes/courses ☐Partnerships ☐Finance ☐Quality ☐Governance ☐Health and safety ☐Facilities ☒IT and Innovation ☐MIS ☐Admissions ☐Teaching and learning ☐Personnel
Audience [select ALL that apply]	☒Employees ☒Learners ☐Partners ☐Suppliers

Information Security Policy

APPENDICES

APPENDIX 1

1. Retention of Data

Type of Data	Suggested Retention Period	Reason
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References and potential litigation
Application forms / interview notes	At least 6 months from the date of the interviews	Time limits in litigation
Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from the date of redundancies	Limitation Act 1980
Income Tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate	Income tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As above	Statutory Sick Pay (General) Regulations 1982
Wages and Salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	RIDDOR 1985
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1994	40 years	COSHHR1994
Student records, including academic achievements and conduct	At least 6 years from the date the learner leaves the College, in case of litigation for negligence At least 10 years for personal and academic references, with the agreement of the learner	Limitation period for negligence

APPENDIX 2

2. Standard Request Form for Access to Data

I …….. wish to have access to either:

1. All the data that Derwentside College currently has about me, either as part of an automated system or part of a relevant filing system, or
2. Data that Derwentside College has about me in the following categories:

    - Academic marks or course work details
    - Academic or employment references
    - Disciplinary records
    - Health and medical matters
    - Political, religious, or trade union information
    - Any statements of opinion about my abilities or performance
    - Personal details including name, address, DOB, etc.
    - Other information

(Please tick as appropriate)

Signed _____

Dated _____