Cardiff and Vale College
Coleg Caerdydd a'r Fro

Information Security Policy for The Quality Skills Alliance

Scope and Purpose of Policy

This policy is underpinned by the Group's vision – Inspirational, Inclusive and Influential and will support our work towards the key drivers of Quality, Efficiency and Growth. The policy will incorporate the following principles:

- Those who access Cardiff and Vale College Group must be **free from discrimination**.
- Learners will be supported to **enable** them to achieve their **potential** whilst in learning, in an environment which removes or minimises disadvantage, takes steps to meet their needs and which encourages participation.
- We will support learners to develop the skills they need to **progress** successfully through their lives.

The purpose of this policy is to ensure the protection of all Cardiff and Vale College Work Based Learning (CAVC WBL) Information Systems, Contract Assets and customer data and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems and assets.

This policy is applicable to, and will be communicated to, all staff and third parties who interact with information held by the CAVC WBL and the information systems used to store and process it.

Policy Statement

In the provision of its services, CAVC WBL will interact with a variety of information assets, with various degrees of confidentiality. They will also be required to comply with statutory and regulatory legislation, and other applicable requirements to which they subscribe (contractually and voluntary). CAVC WBL will:

- Provide a safe and secure information systems working environment for staff, students and any other authorised users.

- Ensure all CAVC WBL's authorised users understand and comply with this policy and any other associated policies.

- Ensure all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

- Protect CAVC WBL, its partners and the Contract from liability or damage through the misuse of its IT facilities.

- Respond to feedback and update as appropriate, initiating a cycle of continuous improvement.

- Provide interested parties with the assurance that information is being 'handled' appropriately.

- Implement an effective Information Security Management System (ISMS) that complies with ISO 27001:2013.

- Ensure the ISMS can manage the information Assets providing assurance of its confidentiality, integrity and availability.

- Continually improve their ISMS and through a number of Information Security Objectives. These will be identified from monitoring the performance of the ISMS.

- Review outputs from regular Risk and Opportunity Assessments, in cooperation with other interested parties.

- Abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements.

Responsibilities

The Governing Body will be responsible for ensuring that:

- The Policy is reviewed on a regular basis (as per the policy terms of review) and appropriate advice is given on content. The Main Board approves the policy.

The Principal will be responsible for ensuring that:

- The College's Information Security Policy and procedures are fully implemented and followed by staff.
- Sufficient resource is allocated to this area.

The Senior Planning Group will be responsible for:

- Reviewing this Policy and the attached procedures.
- Monitoring the application of the procedures, supporting staff to adhere to the policy and responding effectively to any areas of concern.
- Ensuring that relevant college procedures and practices e.g. admissions, tutorial etc embed IT security procedures.

The Director of Information Services and Information Technology will be responsible for:

- Maintaining the currency of this policy and associated procedures.
- Ensuring the allocation of appropriate resources to meet the requirements of the policy and associated procedures.

The Dean of Quality Improvement is responsible for:

- Providing appropriate training and development.
- Appropriate steps are taken to monitor data linked to this policy and that this data is used to inform and improve practice.

All Staff are responsible for:

- Treating all learners with dignity and respect, to ensure their own conduct does not cause offence or misunderstanding.
- Being aware of this policy and the procedures and working in a way that does not contravene their contents.
- Working within the requirements of Data Protection and GDPR.
- Communicating effectively with staff to ensure the needs of learners are met.
- Attending CPD events on aspects relevant to the success of this policy and associated procedures.

Learners are responsible for:

- Attending induction and tutorial sessions to ensure they are aware of the policy and the opportunities it raises.
- Following procedures related to this policy; specifically reporting concerns.
- Providing feedback on the policy in learner focus groups and via other opportunities.

Legislation and Guidance

- The Computer Misuse Act 1990
- Data Protection Act 2018
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2016
- Defamation Act 2013
- Obscene Publications Act 1959
- Protection of Children Act 1978
- Criminal Justice Act 2003
- Digital Economy Act 2017
- General Data Protection Regulation 2018
- Coronavirus Act 2020 Wales 2020

This is a non – exhaustive list and a summary of the legislation, regulatory and contractual obligations can be found in the Information Security Procedure (ISMS01)

Equality and Diversity Statement

In accordance with College procedures, an Equality Impact Assessment was undertaken for this policy.

Health and Safety Implications

Health and safety legislation must be considered in relation to Disclosure as we need to be able to ensure the safety of staff and students.

Welsh Language Standards

This policy does not affect the Welsh language negatively. In accordance with College procedures, this Policy was written with consideration of the impact of individuals as per the Welsh Language Standards.

Linked Policies

Information Security Management System Manual (ISMS00)

Linked Procedures

Information Security Procedure	ISMS01
Access Control Procedure	ISMS02
Anti-virus software Procedure	ISMS03
Application Control Procedure	ISMS04
Decommissioning Procedure	ISMS05
Clear Desk Procedure	ISMS06
Document Control Procedure	ISMS07
Remote Working Procedure	ISMS08
Cryptography Procedure	ISMS09
Monitoring and Logging Procedure	ISMS10
User Account Conditions Procedure	ISMS11
CAVC Forensic Readiness Procedure	ISMS12
Audit of the Management System Procedure	ISMS13
Physical Security Procedure	ISMS19
Document Classification	ISMS20
Acceptable Use Procedure	ISMS21

Approval, Change and Review

This policy is reviewed every 2 years.

Location and Access to the Policy

This is available on the Work Based Learning network drive and mat be out of date if printed.

NOTE: A copy of our ISMS policy is displayed in the work-based learning premises in Barry

Date approved: **January 2017**

Approved by: **CQSA**

Review date: **November 2022**

Responsible Manager: Director ITIS

Executive Lead: Chief Operating Officer

Accessible to Students: : Yes

Revision No:	2
Last Revision Date:	11/20
Next Revision Date	11/22