DATA PROTECTION POLICY

Introduction:

This Data Protection Policy has been developed for the collective Together We Can Succeed (TWCS) organisational consortium of Community Interest Companies. All policies and regulations contained herein apply equally across all three Community Interest Companies identified within this consortium, namely Transferable Skills Training (South West), Work Skills South West and Battling-On.

1. PURPOSE

1.1 TWCS CICs collect and process large volumes of information. In addition to discharging its obligations to protect data belonging to individuals, the organisation recognises that maintaining the integrity and security of personal, commercial and intellectual information is critical to its continued success.

1.2 The purpose of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or operated by TWCS CICs and to ensure compliance with legislation where that is relevant. This will be achieved through:

- Protecting information assets under the control of the organisation
- Describing the principles of security and ensuring that all members of staff fully understand their own responsibilities
- Embedding a consistent approach to information security as an integral part of day to day business
- Ensuring that members of staff are aware of, and fully comply with, relevant legislation

1.3 The policy aims to ensure that:

- Access to data and information systems is confined to those with appropriate authority to preserve commercial and personal confidentiality
- The ability to append, amend and delete data is subject to appropriate controls to preserve the quality and integrity of information
- Information is available to authorised personnel when and where it is needed

1.4 This policy applies to all information, information systems, networks, applications locations and users of TWCS CICs or supplied under contract to it.

2. POLICY

2.1 The Senior Management Team member responsible for oversight of this policy is the Data Protection Officer. He/She is responsible for the authoring, maintenance and operation of the policy, and for monitoring, documenting and communicating information security requirements throughout the organisation.

2.2 The Senior Manager is responsible for the standards of physical security and operational practices applied to information which is under their control and that of their staff.

2.3 All employees must comply with information security procedures in support of the maintenance of data confidentiality and data integrity.

2.4 Managers are responsible for ensuring that every individual working under their supervision is aware of:

- The information security policies and practices applicable to their work areas.
- Their personal responsibilities for information security
- How to access advice on information security matters

2.5 Each member of staff is responsible for the operational security of the information systems they use.

2.6 System users must not use their account to access organisation information systems for any purpose not directly associated with the discharge of their duties on behalf of the organisation.

2.7 Each system user must comply with the security requirements that are currently in force, and must work with due regard for the confidentiality, integrity and availability of the information to which they have access.

2.8 Where information is processed on behalf of the organisation by third-party organisations, a Data Processing Agreement must be in place before access is granted.

2.9 Where information is shared with third-party organisations, an appropriate agreement must be in place before any transfer takes place.

2.10 Where information is required to be shared with a government agency, the organisation will adhere to the information security arrangements provided by that agency in respect of the data transfer.

3. TECHNICAL POLICY

3.1 The architecture of organisational ICT systems will be devised to balance functionality, cost and security risk as directed by the Senior Management Team as appropriate.

3.2 Network, server and storage environments will be configured according to manufacturers' best practice.

3.3 Proprietary line of business systems (HR, Finance etc.) will be configured according to manufacturers' best practice and with due regard to the risks inherent in the organisation's user-base.

3.4 Firmware, Operating Systems and Applications will be maintained at the optimum version/patch levels to balance reliability with security.

3.5 User access will be granted and withdrawn according to established procedure by the appropriate system administrator.

3.6 Employees' privileges over datasets will be assigned according to their job-role. Privileges will be limited to those records and attributes required for the effective discharge of each user's function within the college.

3.7 Where users are permitted to bring their own device, connection to organisational systems will be via the WiFi service and be subject to the standard controls at the perimeter of the internal network.

3.8 Users connecting their own devices to the organisation's services must agree to terms which include the remote erasure of Battling On data from the device if the organisation considers that such data may become compromised.

3.9 Personal data stored on mobile, removable and portable devices including USB flash drives, laptops and tablets must be encrypted to an agreed standard.

4. IMPLEMENTATION

4.1 Management of Security

4.1.1 Senior Management Team responsibility for information security resides with the Data Protection Officer.

4.1.2 Heads of department must ensure that the information processing procedures and practices, followed by them and their staff, meet the standards expressed in this policy.

4.2 Information Security Awareness Training

4.2.1 Information security awareness training will be included in the staff induction process.

4.2.2 Information security guidance and resources will be made available in the main office.

4.2.3 An ongoing awareness programme will be established and maintained to ensure that staff awareness is refreshed and updated as necessary.

4.3 Contracts of Employment

4.3.1 All contracts of employment will contain a confidentiality clause.

4.3.2 Information security expectations upon staff will be included within appropriate job descriptions.

4.4 System Administration Standards

4.4.1 Employees whose role requires that they are granted extended administration privileges across one or more systems must work in accordance with the Code of Practice for Systems Administrators.

4.4.2 Wherever practical, system administration duties should be segregated from day to day operations.

4.5 Access Controls

4.5.1 Only authorised personnel who have a justified and approved business need will be given access to business systems or information storage locations.

4.5.2 Access to personal data will be limited to that needed by individual employees to discharge their job effectively.

4.6 Computer Systems Access Control

4.6.1 Access to computer facilities will be restricted to authorised members of the organisation.

4.6.2 The standard of authentication required for access to the organisation's systems will be determined by the Senior Management Team.

4.7 Removable Media

4.7.1 TWCS CICs organisational datasets should not be copied onto removable media unless the transfer is supervised by the Head of Education or the Data Protection Officer. Smaller collections of personal or commercially sensitive data should only be copied onto removable media with the permission of the Head of Education or the Data Protection Officer. Permission should be granted only where there is no alternative secure means of transmission and where the data is protected by encryption.

4.8 Equipment Security

4.8.1 To minimise potential loss or damage, all assets will be protected from physical threats and environmental hazards so far as is practical. Prior to deployment, all removable ICT equipment will be security marked using a unique code.

4.8.2 All redundant and unserviceable ICT equipment must be returned to the main office for secure data destruction and subsequent disposal according to WEEE regulations.

4.9 Protection from Malicious Software

4.9.1 TWCS CICs will deploy software countermeasures and management procedures to protect itself against the threat of malicious software. Technical measures will be maintained to prevent the user-installation of software on the organisation's devices. ICT users breaching the Code of Practice for users of TWCS CICs ICT systems may be subject to disciplinary action.

4.9.2 The organisation will employ security measures to control external threats and internal-users' internet activity.

4.10 Information Risk Assessment

4.10.1 The organisation will maintain a register of risks, including risks to information assets stored on its servers, together with planned control measures. The administrators of information assets stored elsewhere will be responsible for recording and managing risks to which those assets are exposed.

4.11 Information Security Events and Weaknesses

4.11.1 All information security events will be investigated to establish their cause and impacts with a view to avoiding similar events.

4.11.2 The Data Protection Officer will maintain a protocol for the investigation and reporting of information security events.

4.12 Monitoring System Access and Use

4.12.1 TWCS CICs reserve the right to investigate activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000), together with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, permit monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or out to be achieved by persons using the system
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system

4.12.2 TWCS CICs may also process personal and communications data where this is necessary for the discharge of its statutory duties, for example in respect of the prevention of radicalisation.

4.12.3 Any monitoring will be undertaken in accordance with the above legislation and the Human Rights Act

4.13 Currency of Information Systems

4.13.1 TWCS CICs will ensure that all information systems, applications and networks are maintained according to manufacturers' best practice. Workstation Operating Systems and applications will be maintained at the latest patch level according to established procedure and subject to testing where appropriate.

4.14 Intellectual Property Rights

4.14.1 TWCS CICs will ensure that all information products are properly licensed and approved. Users will not install software on the organisation's property without permission from the Data Protection Officer. ICT users breaching the Code of Practice may be subject to disciplinary action.

4.15 Business Continuity and Disaster Recovery Plans

4.15.1 The organisation will maintain a data backup regime, in respect of locally-hosted services.

4.15.2 The organisation will be responsible for the recovery of mission-critical, locally-hosted, information, applications, systems and networks in the event of a disaster.

4.15.3 The administrators of Cloud-hosted services will be responsible for ensuring that appropriate back-up and recovery provision is in place.

4.16 Relevant Legislation

4.16.1 TWCS CICs are obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of the organisation, who may be held personally accountable for any breaches of information security for which they may be held responsible. TWCS CICs will comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)
- Freedom of Information Act (2000)
- Counter-Terrorism and Security Act (2015)

This policy should be read in conjunction with the Privacy Notices for Staff and Learners.

REVIEW HISTORY

April 6th 2018 Policy written, Helena Drawer

Last review 13 Dec 19 by Rick Stead

NEXT REVIEW DATE

Next Review:- Dec 2020