# Information Security Policy

| | |
|---|---|
| **Board Approved Date** | March 2022 |
| **Version** | 1.4 |
| **Author Initials** | ZW & TD (SW) |
| **Review Date** | February 2023 |

**Amendments**

| Policy Date | New Version Number | Summary of change | Comments |
|---|---|---|---|
| March 2021 | 1.3 | 13 Remote Learning | |
| February 2022 | 1.4 | 6.4 and 8.1 updated | |
| | | | |
| | | | |
| | | | |



NON CONTRACTUAL POLICY

## Contents

1. Introduction ..... 4
2. Purpose and Statement of Policy ..... 4
3. Legal Framework for Information Security ..... 4
4. Information Security Definition ..... 5
5. Risk Management ..... 5
6. Computer and Network Security ..... 5
7. Security from Malware and Intrusion ..... 6
8. User Authentication and Access Management ..... 7
9. Physical Security ..... 7
10. Asset Management ..... 8
11. Monitoring and Acceptable Use ..... 8
12. Home and Mobile Working ..... 8
13. Handling of Personal Data ..... 9
14. Third Party ..... 9
15. Breaches of the Information Security Policy ..... 9
16. Information Security Incident Management ..... 10
17. Review of policy ..... 10



NON CONTRACTUAL POLICY

## 1. Introduction

1.1 Education South West (ESW) is committed to ensure the security of all information that it holds and to implement the highest standards of information security in order to achieve this.

1.2 Information is one of the Trusts most important assets. The Information Security Policy provides a framework by which we are able to clarify our information security procedures.

## 2. Purpose and Statement of Policy

2.1 This policy provides a framework of four levels of information security for all ESW information systems (including but not limited to all Cloud environments commissioned or run by ESW, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risk associated with the theft, loss, misuse, damage or abuse of these systems.

2.2 The purpose of this document is to specify ESW's requirements with respect to information security, specifically:

- To protect the Trust's Information and subsequently to protect the Trust's reputation;
- To enable secure information sharing to deliver services;
- To protect the Trust from legal liability and inappropriate use;
- To encourage consistent and professional use of information and systems;
- To ensure everyone is clear about their roles in using and protecting information;
- To maintain awareness of information security;
- To protect the Trust's employees;
- NOT to constrain reasonable use of information in support of normal business activities of the Trust and its schools.

## 3. Legal Framework for Information Security

3.1 All employees and Directors, Governors, and students of the Trust have a responsibility regarding the legal use of information. The following laws and legal rules govern how information is handled: -

- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018 (encompassing GDPR)
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Human Rights Act 1998
- Protection of Children Act 1999
- Indecent display (Control) Act 1981
- Theft Act 1978
- Obscene Publications Act 1984

- Copyright, Designs and Patents Act 1998
- Health and Safety at Work Act 1974
- Privacy and Electronic Communications Regulations 2003
- Digital Economy Act 2010
- Counter-Terrorism and Security Act 2015

## 4. Information Security Definition

4.1 Information comes in many forms. It can be stored on computers, sent across networks, printed out, written, spoken and displayed.

4.2 The International Standard ISO/IEC 27001:2005 specification for information security management defines information security as protecting three aspects of information:

- **Confidentiality** - information is accessible only to those authorised to have access
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods
- **Availability** - only authorised users have access to information and associated resources when required.

## 5. Risk Management

5.1 Much of the information held by the Trust is confidential and sensitive in nature. Therefore, it is necessary for all information systems to have appropriate protection against adverse events (accidental or malicious) which may put at risk the activities of the Trust or protection of the information held.

5.2 This is put into practice through appropriate controls, which are a combination of policies, procedures, standards, guidelines, common sense and physical or hardware/software measures.

5.3 The framework for these control measures is outlined over the next sections of the policy.

## 6. Computer and Network Security

6.1 Network monitoring and log activity is required to provide assurance that only authorised persons are accessing the data the Trust is responsible for. Where a significant risk has been identified, automatic monitoring takes place. For example, files created on the file server with a file name string that matches a known ransomware, generate an automatic email alert to the IT helpdesk and each event individually investigated.

6.2 The Trust also ensures that procurement and implementation of new or upgraded software is carefully planned. All software installations are controlled following prescribed security protocols. End users can only install software from the software library or if an exception has been made, otherwise all software installations must be installed by an

administrator. Only authorised individuals from the ESW IT Services Team perform software updates/patches.

6.3 Information security risks associated with implementations (6.2) are mitigated using a combination of procedural and technical controls. To prevent copyright infringements and protect all information systems, the Trust closely monitors all software renewals. Software cannot be installed onto any PC or laptop within the Trust by unauthorised staff or any students.

6.4 The Trust ensures that backup and system recovery measures are in place. All servers are backed up daily with the backups for every site stored in a location separate from the production servers. Offsite backups are delivered over an encrypted connection to maintain security. Offsite backup repositories are located at Teign School, Coombeshead Academy, and Kingsbridge Community College. Offsite backups are stored at one of these locations, ensuring that the back-up is not store at the site of the production servers, i.e. Kingsbridge backup is not stored at Kingsbridge.

6.5 When permanently disposing of equipment containing storage media all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site. Damaged storage devices are assumed to contain sensitive data and undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded.

6.6 Email is a significant source of risk of information security breach, through malware and phishing, and also loss of information through human error, or lack of awareness of appropriate communication methods for different types of data.

6.7 All emails sent between ESW schools are encrypted using TLS encryption. Any emails that are sent without TLS encryption will be rejected by the server and not sent. Users are able to encrypt messages containing sensitive information to outside the organisation by using OME (Office 365 Message Encryption) which is a service built into Azure Rights Management (Azure RMS). The Trust uses Office 365 accounts which are linked to Active Directory enabling passwords to be synchronised.

## 7. Security from Malware and Intrusion

7.1 Systems are protected from the outside world with a secure firewall that is regularly updated to resolve new threats.

7.2 Operating systems and other software and hardware systems are patched to meet vendors recommendations in order to protect the Trust and its schools against vulnerabilities. Malware protection is installed on all endpoint and server devices. Vulnerability scans are regularly run against all systems to find any other known vulnerabilities.

Spam and phishing filters are in place and updated to reduce the risk of phishing attacks.

## 8. User Authentication and Access Management

8.1 To comply with the most fundamental principles of information security, users with access to systems and data are authenticated. All users who access a computer system within the Trust have a legitimate user login and password. Each user has a secure password that meets a minimum password complexity standard and which automatically renews every 90 days. The Trust expects all users (staff and students) to adhere to the ESW Acceptable Use of ICT Policy and the ESW Staff Acceptable Use of IT Agreement.

8.2 Staff users are required to enrol a second form of authentication for systems that support 'two factor authentication' or 'multi factor authentication'. All data stored on the Trust's IT Systems, as well as paper records, are only available to staff with a legitimate need for access. The IT Manager, in accordance with senior leadership requests, ensures that all members of staff are granted levels of access to IT Systems that are appropriate, considering their job role, responsibilities, and any special security requirements.

8.3 User accounts are reviewed regularly and a process is in place to ensure that the accounts of staff, students and governors that leave the organisation are disabled as soon as they have left.

## 9. Physical Security

9.1 Physical security and access control measures are in place in areas and offices where sensitive or critical information is processed. Appropriate building security measures such as entry key pads, alarms etc are used. Only authorised persons are allowed in Trust server rooms which are locked when not in use.

9.2 Paper records and documents containing personal information, sensitive personal information, and confidential information are locked away securely when not in use either in locked classrooms, offices or store rooms or lockable cupboards provided. This is in accordance with the ESW Data Protection Policy.

9.3 All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy and the ESW Data Protection Policy, ESW Freedom of Information Policy and the ESW Staff Acceptable IT Use Agreement.

9.4 Visitors to the school are required to sign in and out, to wear identification badges whilst in one of the Trust's schools and are, where appropriate, accompanied.

9.5 Building security systems are in place and include key pad entry systems, CCTV and intruder alarms.

9.6 Production server rooms have one primary air conditioning unit and one backup air conditioning unit. Temperature thresholds are set on production servers to shut down in the event of complete air conditioning failure. Backup server rooms are temperature controlled using air conditioning.

## 10. Asset Management

10.1 All data stored on our IT systems is classified appropriately and detailed in the Trust Information Asset Register (IAR). All data deemed confidential, or classed as personal data or sensitive personal data under the Data Protection Policy must be handled appropriately and is also detailed on the IAR.

10.2 All information assets are 'owned' by the Trust and a Data Owner who is in charge of each record, their secure retention and appropriate disposal. This is detailed in the IAR alongside the ESW Records Retention Schedule.

10.3 For the asset management of the physical IT assets, the Trust uses Asset Tiger which allows the assets to be recorded against each user. Shared mobile assets and fixed devices are assigned to a school and department. When a member of staff leaves the organisation the asset register is checked to ensure all company equipment is returned.

## 11. Monitoring and Acceptable Use

11.1 To protect users and data from harm caused by misuse of IT Systems, definitions of acceptable and unacceptable behaviour is defined in the ESW Acceptable Use of ICT Policy and the ESW Staff Acceptable Use of IT Agreement. All staff are required to read and acknowledge acceptance of the ESW Staff Acceptable Use of IT Agreement.

## 12. Home and Mobile Working

12.1 In accordance with the ESW Data Protection Policy, all staff home and mobile working, are made aware of the appropriate technical and practical measures to take to maintain the continued security and confidentiality of that information.

12.2 With the proliferation of mobile devices (smartphones, tablets and laptops) it is important that the risk these devices present with respect to storage of data, transferability of data and security over the device is understood by staff and appropriate training and policy protocols put in place to prevent data loss, release, or unauthorised access.

12.3 Staff laptops are setup with an encrypted connection back to the users main site using Microsoft Direct Access. Staff and Students are also

able to access files stored on the organisation file server using a secure web interface provided using Foldr.

12.4 The ESW Staff Acceptable Use of IT Agreement details expectations in relation to all users having access to Microsoft OneDrive cloud storage and the use of mobiles, smart phones and tablets for work purposes.

## 13. Remote Learning

13.1 Students and staff use organisation approved systems, such as Microsoft Teams and/or Seesaw, with managed accounts to enable the process of remote learning.

13.2 Laptops issues by the school (trust) to students must be managed with always on VPN technology, such as MS Direct Access.

## 14. Handling of Personal Data

14.1 All handling of personal data is in accordance with the Trust Data Protection Policy and Article 5 of the GDPR. The Trust processes this information in accordance with its Workforce and Pupil Privacy Notices.

## 15. Third Party

15.1 Where a third party is asked to process data on behalf of the Academy, the Trust reviews the third party's information security arrangements and are provided with written authorisation for the processing to commence. This is achieved via the GDPRiS system which assesses any associated risks and highlights issues prior to implementation.

## 16. Breaches of the Information Security Policy

16.1 Failure to ensure adequate security and protection of information held by the Trust may lead to legal action. Legal action under data protection legislation could lead to a fine for the Trust or for an individual. For more detail on data breaches please refer to the ESW Data Protection Policy

16.2 This policy applies to all members of staff, including temporary workers, as well as other contractors, volunteers, student teachers, governors, directors and all third parties authorised to use the IT systems. All staff are required to familiarise themselves with its content and comply with the provisions contained in it. All non-Trust staff such as supply teachers, contractors, volunteers will be given this policy by their main school contact and will be asked to acknowledge that they have read and understood it. Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action.

## 17. Information Security Incident Management

17.1 Where there has been any breach of information security, the ESW Data Protection Officer (and ESW IT Manager for IT incidents) must be informed immediately. The Trust record and maintain a register of all Information Security incidents which are logged in accordance with the Data Protection Act 2018. A summary of all incidents is reported to the ESW Board six times each year.

17.2 The Trust has in place a Business Continuity Plan. The Plan details a process to react to and counteract the interruption of Trust business caused by major service failure. This includes major IT failure. Refer to ESW Business Continuity Plan for more information.

## 18. Review of policy

18.1 This policy is reviewed every twelve months by the Trust in consultation with the recognised trade unions. We will monitor the application and outcomes of this policy to ensure it is working effectively.