INVICTUS
Education Trust

INVICTUS EDUCATION TRUST

GDPR INFORMATION SECURITY POLICY

Approved by Board of Trustees
25 May 2021

To be reviewed by Board of Trustee
April 2023

Document Provenance

GDPR Information Security Policy	
Committee Approval Level	Board of Trustees
Policy Author/Responsibility	Chief Operating Officer – Julie Duern
Policy First Implemented	July 2018
Frequency of Review	Every 2 Years
Next Review Date	April 2021
Policy Approved by Committee	25 May 2021
Next Review Date	April 2023

Contents **Page**

1. Introduction

Invictus Education Trust has an extensive and robust Information Security Program that consists of a vast array of policies, procedures, controls and measures. This Information Security Policy is the foundation of this program and ties together all other policies as they relate to information security and data protection.

The Trust's Information Security Policy covers all aspects of how we identify, secure, manage, use and dispose of information and physical assets as well as acceptable use protocols, remote access, password and encryptions. To ensure that the importance of each information security area is not missed or vague, we use separate policies and procedures for each information security area and where applicable, reference these external policies in this document.

All information security policies and procedures should be read and referred to in conjunction with each other, as their meaning, controls and measures often overlap. The policies and documents that form part of the Trust's Information Security Programme are:

- Information Security Policy
- Risk Assessment Policy & Procedures
- Business Continuity Plan
- Access Control & Password Policy
- Data Retention & Erasure Policy
- Data Protection Policy & Procedure
- Data Breach Policy

2. Policy Statement

Information and physical security is the protection of the information and data that the Trust creates, handles and processes in terms of its confidentiality, integrity and availability from an ever-growing number and wider variety of threats, internally and externally. Information security is extremely important as an enabling mechanism for information sharing between other parties.

The Trust is committed to preserving Information Security of all physical, electronic and intangible information assets across the schools/business, including, but not limited to all operations and activities.

We aim to provide information and physical security to:

- Protect Student/Parent & Employee Data
- Protect Third Party and Client Data
- Preserve the integrity of the Trust and our reputation
- Comply with legal, statutory, regulatory and contractual compliance
- Ensure business continuity and minimum disruption
- Minimise and mitigate against business risk

3. Purpose

The purpose of this document is to provide the Trust's statement of intent on how it provides information security and to reassure all parties involved with the Trust that their information is protected and secure from risk at all times.

The information the Trust manages will be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.

4. Scope

This policy applies to all staff within the Trust *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Trust),* and pertains to the processing of personal information. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5. Objectives

The Trust has adopted the below set of principles and objectives to outline and underpin this, policy and any associated information security procedures:

- Information will be protected in line with all our data protection and security policies and the associated regulations and legislation, notably those relating to data protection, human rights and the Freedom of Information Act.

- All information assets will be documented on an Information Asset Register (IAR) by the Network Managers and will be assigned a nominated owner who will be responsible for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect it

- All information will be classified according to an appropriate level of security and will only be made available solely to those who have a legitimate need for access and who are authorised to do so

- It is the responsibility of all individuals who have been granted access to any personal or confidential information, to handle it appropriately in accordance with its classification and the data protection principles

- Information will be protected against unauthorised access and we will use encryption methods as set out in the above objectives in this policy

- Compliance with this Information Security and associated policies will be enforced and failure to follow either this policy or its associated procedures will result in disciplinary action

The Network Managers have the overall responsibility for the governance and maintenance of this document and its associated procedures and will review it regularly to ensure this it is still fit for purpose and compliant with all legal, statutory and regulatory requirements and rules.

6. Procedures & Guidelines

6.1 Security Classification

Each information asset will be assigned a security classification by the asset owner or Information Security Officer, which will reflect the sensitivity of the asset. Classifications will be listed on the Information Asset Register.

6.2 Access to Information

Staff at the Trust will only be granted access to the information that they need to fulfil their role within the organisation. Staff who have been granted access must not pass on information to others unless they have also been granted access through appropriate authorisation. Refer to the Trust's Access Management Policy for protocols and more information.

6.3 Secure Disposal of Information

Care needs to be taken to ensure that information assets are disposed of safely and securely and confidential paper waste must be disposed of in accordance with relevant procedures on secure waste disposal. Where, an external shredding service provider is employed, secure paper disposal bins/bags are located in each office, and used in all instances of confidential paper disposal.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the Trust, unless an approved disposal contractor undertakes the disposal under contract.

In cases where a storage system *(for example a computer disc)* is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. Refer to the Trust's Retention Policy for protocols and more information.

6.4 Information on Desks, Screens and Printers

Members of staff who handle confidential paper documents should respond appropriately to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that unauthorised persons cannot view them and all computers should be locked while unattended.

6.5 Data Encryption

Encryption methods are always used to protect confidential and personal information within the Trust and when transmitted across data networks. We also use encryption methods when accessing the Trust's network services, which requires authentication of valid credentials *(usernames and passwords)*.

Where confidential data is stored on mobile devices *(for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders)* the devices themselves are be encrypted (*using "full disk" encryption*), irrespective of ownership. Where strictly confidential data is stored in public, cloud based storage facilities the data must be encrypted prior to storing to ensure that it is not possible for the cloud service provider to decrypt the data.

Where data is subject to an agreement with an external organisation, the data should be handled *(stored, transmitted or processed)* in accordance with the organisation has specified encryption requirements.

Where there is a requirement to remove or transfer personal information outside of the Trust, it is always kept in an encrypted format. Encryption is used whenever appropriate on all remote access connections to the organisation's network and resources. The Trust also has documented protocols for the management and use of electronic keys, with a view to controlling both the encryption and decryption of confidential and sensitive information.

All confidential and restricted information transmitted via email is encrypted. Where a secret key is provided to decrypt, this is done so in a separate format to the original email.

6.5.1 Encryption Keys

<u>Definitions</u>

- *Encryption:* This is the process of locking up (*encrypting*) information using cryptography. Such information appears illegible if access, unless a corresponding key is used to decrypt the data.

- *Decryption:* The process of unlocking the encrypted information via a key.

The Trust utilises both asymmetric and symmetric key encryption algorithms, dependant on the systems, purpose and information. The type of encryption is decided by the Network Managers after assessing the requirements of the information and transfer.

- *Asymmetric Key Encryption Algorithms:* A type of encryption algorithm whereby two different keys are used. One key is for encrypting the information and the other for decrypting. This type is also known as public-key encryption.

- Symmetric Algorithms: also referred to as *"secret key encryption",* and use the same key for both encryption and decryption.

6.5.2 Approved Encryption Algorithms and Protocols

The Trust uses a variety of encryption methods dependant on the nature of the information being, stored or transferred its location, and its use. Below are the standard and acceptable forms of encryption used by the Trust.

Symmetric Key Encryption Algorithms

- Triple Data Encryption Standard (3DES)- Minimum encryption key length of 168 bits
- Advanced Encryption Standard (AES)- Minimum encryption key length of 256 bits

Asymmetric Key Encryption Algorithms

- Digital Signature Standard (DSS)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

Encryption Protocols

- IPSEC *(IP Security)*
- SSH (*Secure Shell)*
- TLS (*Transport Layer Security)*
- HTTPS – Secure Hypertext Transfer Protocol

6.5.3 Key Use & Protocols

Encryption key management is fully automated and all private keys are kept secure, restricted and confidential. Whilst keys are in transit and/or storage, they are always encrypted.

Due to their nature, when the Trust uses symmetric encryption key algorithms, there is a requirement to share the secret key with the recipient. Protecting and securing the key for sharing is paramount to protecting the information the key encrypts, and so encrypting the key itself is a mandatory requirement. During distribution and transfer, the symmetric encryption keys are always encrypted using a stronger algorithm with a key of the longest key length for that algorithm.

The Trust's aim when encrypting secret keys is to afford them a higher, more stringent level of protection than the encryption used to protect the data. When keys are at rest, they are again secured with encryption methods, equal to or higher than the existing encryption level.

Where asymmetric algorithms are used, the public key is passed to the certificate authority to be included in the digital certificate that will be issued to the end user. Once the digital certificate is issued, it is then made available to all relevant parties. The corresponding private key is only made available to the end user who is in receipt of the corresponding digital certificate.

6.6 Remote Access

It is the responsibility of all the Trust's employees with remote access privileges to the Trusts network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Trust.

- Secure remote access must be strictly controlled
- Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases
- At no time, should any of the Trusts employees provide their login or email password to anyone else
- The Trust's employees with remote access privileges must ensure that their Trust owned or personal computer/workstation, which is remotely connected to the Trust's network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.
- All hosts that are connected to the Trust's internal networks via remote access must use the most up-to-date anti-virus software

6.7 Firewalls & Malware

Invictus Education Trust understands that adequate and effective firewalls, malware and protected gateways are one of the main and first lines of defence against breaches via the internet and our networks.

We utilise configured firewalls and have daily anti-virus applications running on all computers, networks and servers. The Network Managers are responsible for checking the log of all scans and for keeping these applications updated and compliant.

Systems are regularly scanned and assessed for unused and outdated software, with the aim of reducing potential vulnerabilities, and we routinely remove such software and services from our devices where applicable.

The Network Managers also have full responsibility for ensuring that the latest application and software updates and/or patches are downloaded and installed, keeping our security tools current and effective. Security software is reviewed and updated monthly, or sooner where updates or patches have been released.

7. Security Breach Management

7.1 Introduction

The Trust's definition of a breach for the purposes of this and related documents is a divergence from any standard operating procedure (SOP), which causes a failure to meet the required compliance standards as laid out by our own compliance program objectives and/or those of any regulatory body.
Compliance in this document means any area of business that is subject to rules, laws or guidelines set out by a third party which are to be followed and which, when breached, could cause emotional, reputational or financial damage to a third party.

7.2 Breach Management Approach

The Trust has robust objectives and controls in place for preventing security breaches and for managing them if they do occur. Due to the nature of our business, the Trust processed and stores a vast amount

of personal information and confidential client data and as such, require a structured and documented breach incident program to mitigate the impact of any breaches. Whilst we take every care with our systems, security and information, risks still exist when using technology and being reliant on human intervention, necessitating defined measures and protocols for handling any breaches.

We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary, however should there be any compliance breaches, we are fully prepared to identify, investigate manage and mitigate with immediate effect and to reduce risks and impact.

The Trust has the below objectives, with regards to Breach Management:

- To maintain a robust set of compliance procedures which aim to mitigate against any risk and provide a compliant environment for trading and business activities

- To develop and implement strict compliance breach and risk assessment procedures that all staff are aware of and can follow

- To ensure that any compliance breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks

- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring

- To use the Compliance Breach Incident Form for all breaches, regardless of severity so that any patterns in causes can be identified and corrected

- To comply with regulating bodies and laws on compliance breach methods, procedures and controls

- To protect consumers, clients and staff – including their data, information and identity

Please refer to our Data Breach Policy & Procedures for further details.

8. Responsibilities

All information users within the Trust are responsible for protecting and ensuring the security of the information to which they have access. Managers and staff are responsible for ensuring that all information in their direct work area is managed in conformance with this policy and any subsequent procedures or documents. Staff who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures.

The Trust will ensure that staff do not attempt to gain access to information that is not necessary to hold, know or process and that restrictions and/or encryptions are in place for specific roles within the organisation relating to personal and/or sensitive information.