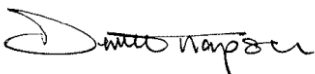


# ETT Data Protection & Information Security Policy

**Signed:** 

**Position:** Chief Executive

**Date:** October 2019

**Review Date:** October 2020

## Introduction

Effective information security is a key priority for the Electrical Training Trust (ETT). ETT recognises that stringent principles of information security must be applied to **all** information it holds. This includes business and commercially sensitive information, and personal data on customers, employees, suppliers, Contractors and citizens.

The specific purpose of this document is to bring together into a single source an overview of the various policies, procedures and structures that have been put in place to ensure the delivery of a safe environment for the handling of all the information and data required by ETT to carry out its responsibilities

## Purpose

ETT regards the lawful and correct treatment of personal information as essential to its successful operations. ETT seeks to foster a culture that values, protects and uses information for the public good through a range of methods and arrangements. The objective of this policy is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System in line with the Data Protection Act 1998 and best practice guidelines from the Information Commissioners Office (ICO).

## Scope

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing). *Please Note: The impact of these guidelines on daily activity should be minimal.* Questions about the proper classification of a specific piece of information should be addressed to your manager.

## Policy

All staff must follow the eight data protection principles of good information handling. These say that personal information must be:

- Fairly and lawfully processed;
- Processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and, where necessary, kept up to date;
- Not kept for longer than is necessary;
- Processed in line with the rights of the individual;
- Kept secure; and
- Not transferred to countries outside the European Economic Area unless the information is adequately protected

Confidential Information will only be available to staff who are directly involved and who need to know the information. Any confidential information will only be used for the purposes that the client intended.

All existing staff, new staff and agents will be vetted and provided with appropriate industry standard training to ensure compliance with the requirements of relevant legislation and the ETT information security policy. If requested by a customer/supplier ETT staff will comply with appropriate confidentiality agreements requested. ETT will process personal data only in accordance with instructions from the client or the individual concerned and in such manner as is necessary for the provision of services including auditing purposes.

Written consent will be gained if transfer of personal data is needed for any reason. ETT may disclose confidential information with prior written notification if requested by Crown Body or any Contracting Authority; consultants of third parties and in line with the National Audit Act 1983 or for the purposes of assisting in the prevention and detection of fraud pursuant to powers inserted in the Audit and Accountability (Northern Ireland) Order 2003 by the Serious Crime Act 2007. ETT will treat all other party's Confidential Information as confidential and safeguard it accordingly; and not disclose the other party's Confidential Information to any other person without the owner's prior written consent. ETT will provide any individual with full cooperation and assistance in relation to any complaint or request made

Any employee found to have violated ETT policy may be subject to disciplinary action, up to and including termination of employment. ETT will ensure that there are sufficient measures in place for the restoration of corrupted or lost data and to inform the client of any corruption loss or degradation.

## **Internal Measures**

### **Appropriate measures to ensure Data Protection and Security**

To remove risk to ETT from an outside business connection. ETT computer use by any unauthorised personnel must be restricted so that, the risk of an attempt to access ETT information, is removed.

### **Malicious Software**

ETT will ensure that the latest versions of anti-virus definitions available [from an industry accepted anti-virus software vendor] are used to check for and delete Malicious Software from the ICT Environment. If Malicious Software is found, ETT shall co-operate with affected parties to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of data, assist each other to mitigate any losses and to restore the services to their desired operating efficiency.

### **Approved Electronic Mail**

Anti-Virus software will be updated daily by members of staff and full system scans carried out on a weekly basis. All email attachments must be scanned prior to opening.

### **Approved Encrypted email and files**

Techniques include the creation of password protection and/ or encryption for any confidential or sensitive information being sent outside ETT. This should be clearly marked as confidential and should be approved by your manager prior to sending.

### **Computers**

Company Information System Resources include, but are not limited to, all computers, their data and programs. ETT computerised data is stored on a secured central server and is backed up onto daily backup tapes which are changed every day and placed into a fireproof safe. Information held on the ETT server is also backed up onto an external hard drive.

### **Data Storage & Business Continuity and Disaster Recovery Plan**

All hard copy information including registration forms, training contracts and personal information on apprentices is stored in an approved high security storage environment. Operating to BS7799 standards these measures include;

- 24 hr / 365 day monitored security access
- High security steel perimeter fencing
- Detached buildings (no party walls)
- Remote control of automatic gate system to vehicle compound
- External CCTV (colour/mono) with full recording and web access
- Infra-red and automatic lighting for camera image clarity
- External and internal door access systems with nominated authority levels
- Insurance approved swipe-card locking systems throughout
- All ground floor windows fitted with high-security steel shutters
- Roof detectors
- All intruder systems are externally monitored via RedCare / G.S.M.

All hard copy data held by ETT can be quickly recalled for any reason with a next day delivery. All client proprietary data will be held in accordance with the client's security policy.

### **Premises**

ETT premises are secured by a PSNI approved grade 5 alarm system by Atlas intruder alarms and makes use of BT Redcare. Redcare is a market-leading specialist in secure, monitored communications services, which help customers to benefit from automated, intelligent decisions and responses. Only a number of limited, authorised key holders have access to the alarm code for the building. The alarm is set every evening by authorised personnel. The premises are also secured by an electronic gate that requires a swipe card to gain entry outside of office hours.

## **Legislation**

ETT will comply at all times with the Data Protection Legislation and shall not perform its obligations under this Agreement in such a way as to cause breach any of its applicable obligations under the Data Protection Legislation.

Legislation, including the Official Secrets Acts 1911 to 1989; the Public Records Act 1923, Data Protection Act 1998, Freedom of Information Act 2000, Computer Misuse Act 1990, Human Rights Act 1998 and Section 182 of the Finance Act 1989 set the legal framework within which ETT must operate and ensure the safe storage and handling of information.

## **Freedom of Information**

ETT acknowledges that it is subject to the requirements of the Code of Practice on Government Information, Freedom of Information Act (2000) (FOIA) and the Environmental Information Regulations and shall assist and cooperate with the Client to enable the Client to comply with its Information disclosure obligations.

In no event shall ETT staff respond directly to a Request for Information unless expressly authorised to do so by the Chief Executive. ETT will take reasonable steps, where appropriate, to give the advanced notice, or failing that, to draw the disclosure to the attention of any third parties after any such disclosure.

## **Intellectual Property**

All Intellectual Property Rights will be respected by ETT for clients and suppliers, including in guidance, specifications, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material.

ETT will ensure that any third party owner of any Intellectual Property Rights that are or which may be used grants to a non-exclusive licence or, if itself a licensee of those rights, shall grant an authorised sub-licence,

ETT will notify the relevant clients/suppliers in writing of any claim or demand brought against ETT for infringement or alleged infringement of any Intellectual Property Right in materials supplied or licensed by the client/ supplier. Any resulting negotiations and any litigation shall be at ETTs expense. In these circumstances ETT shall take due and proper account of the interests of the Client; and shall not settle or compromise any claim without the Client's prior written consent.

## **Credit/ Debit Card Details**

Credit/ debit card payments can be taken over the phone in person and through the organisation's website. There are no card details recorded and no information stored relating to card numbers, CSV etc. Payments taken over the phone are taken immediately so that there is no requirement to record information. The

organisation will ensure to abide by Worldpay PCI guidelines and continue to ensure compliance with PCI standards.



## **Audits**

ETT acknowledges that audits may be carried out by Clients, ETT will provide reasonable co-operation and assistance in relation to any Client audit within the permitted scope of the audit; Reasonable access to ETT and to any equipment used, data analysis or reports in the provision of the Services; and access to Staff

## **Review and Additional Requirements**

The ETT Data Security policy will be revised annually with assistance of approved specialists. As an addition to the information presented in this policy ETT will abide by the following key rules

1. Staff who use a portable device are personally responsible for its safekeeping and for the security of any information it contains.
2. Be very careful with sensitive and personal data. Sensitive data are any documents or e-mails that are, or should be, marked 'RESTRICTED' or 'PROTECT – PERSONAL DATA'. Be specially careful about files which contain large volumes of personal data – e.g. spreadsheets with large lists of personal details or which may identify or relate to a 3<sup>rd</sup> party.
3. If you leave any computer switched on and unattended press Ctrl / Alt / Delete and select 'Lock Computer'.
4. Sensitive or personal data must not be stored on a laptop unless it is encrypted.
5. Sensitive or personal data must not be stored on mobile phones or removable media unless encrypted. Removable media include USB data drives, external hard drives, CDs, or multi-media data storage cards. The only encrypted mobile phone is a Blackberry.
6. During office hours, laptops must not be left unattended unless firmly secured with a cable lock.
7. Outside office hours, laptops that are left in the office must be stored in a suitable locked cabinet. Cable locks are not secure out of hours.
8. Be very careful if you take your laptop or portable device out of the office. Take special care in public, at airport security checks, in cars, in hotel rooms and at conferences or meetings.

9. Encrypted laptops and Blackberries are secure, but you must still take great care of them. First of all they are high-cost and valuable items, but also if they are lost or stolen there will be a perception that sensitive or personal data has been compromised.
10. Exceptions to these rules can only be made in the most exceptional circumstances and then only if approved in writing by the Chief Executive, with a copy to the Information Security Officer.