Shorcontrol Safety	Document Title	**Data Protection & Privacy Policy**		
	Doc. Number	GEN-POL-010	Doc. Owner	General Manager
	Author	Angela Byrne	Revision	Rev. 05
	Reviewed by	Angela Byrne	Approved by	Fiona Spillane
	Next Review Date	26/07/2026	Approved Date	26/07/2025

1. Policy Statement

At Shorcontrol Safety, we are responsible for safeguarding the privacy and rights of individuals in relation to the processing of personal data in all its forms. In the course of our business activities, we are required to collect and use certain types of information including 'personal data' and 'special category data'. At Shorcontrol Safety we are firmly committed to preserving the privacy of all our stakeholders, interested parties, and employees, in accordance with applicable law following the EU General Data Protection Regulation (GDPR).

Shorcontrol Safety's strategy to implement the policy includes awareness training for all managers and employees, with access to high volumes of personal data or special category data and are able to demonstrate competence in their understanding of data privacy. We shall ensure that all employees understand their responsibility to protect personal data in accordance with this policy, any related procedures, and applicable laws.

2. Purpose

The purpose of this policy is to clearly define how Shorcontrol Safety ensure that in carrying out its business activities, manage, handle, use, store and destroy protected data in line with GDPR requirements. It is our commitment to protect the rights and privacy of all individuals whether employees, customers, suppliers, or contractors in accordance with current Data Protection laws and regulations.

3. Scope

The scope of this policy aims to comply with:

- GDPR Data Protection Principles – Data Protection Act 2018

and is applicable to all matters related to the use of the company's website and any other digital information collected by the company, internal processes, all members of Shorcontrol Safety Staff, Tutors, Learners, Subcontractors and Visitors.

4. Definitions

Term	Definition
GDPR **Data Protection Law**	The General Data Protection Regulation 2018 is the regulation within EU law on data protection and privacy.
Personal Data	Information that relates to or can identify a person. Either by itself or together with other available information. It can include: • Name, • Address • Contact details • PPSN • IP/ Internet address • Access cards • CCTV footage, Audio or Audio-visual recordings • Location data

Special Category Data	Sensitive personal data that is subject to additional protection under the GDPR such as: • Ethnic or racial origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data, biometric data • Health information • Sexual orientation
Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processor	The natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Natural Person	Legal terms referring to an individual who has their own legal personality (an individual human being). As opposed to a legal person, of which may be a private or public entity (e.g. business, government department, etc.).

5. General Policy Requirements

5.1 GDPR Data Protection Principles

- The personal data which Shorcontrol Safety collects shall be processed in a manner that is lawful, transparent, and fair.
- Shorcontrol Safety will collect personal data only for specified, explicit, and legitimate purposes.
- The amount of data collected shall be adequate, relevant, and limited to what is necessary for the purpose.
- Shorcontrol Safety shall take reasonable steps to ensure that the personal data collected are accurate and up to date, and that inaccurate data are erased.
- Personal data shall be kept only for the length of time necessary to carry out the purpose for which the data was collected.
- Personal data shall be processed in a manner that ensures appropriate security of the data, including protection from unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5.2 Personal Information

- Personal information is information that can be used to identify individuals.
- All personal information is gathered through phone, email, and hard copy forms.
- Any personal information collected will be used only to provide the services of our organization.

5.3 Data Controllers and Processors

- Upon collecting personal data from a data subject, the controller is required to provide the individual with certain information including:
  - The purpose for which the personal data is intended,
  - The period of time for which the data will be stored,
  - That any personal data supplied allows for Shorcontrol Safety to submit the data to any relevant awarding body regarding accreditation, training, awards, and certification.
- All data must be processed in accordance with the GDPR, and the processor will ensure the rights of the data subjects.
- Data Processors should maintain a record of processing activities under their responsibility which shall include:
  - Name and contact details of controller & processor,
  - Purpose of processing data,
  - Description of the categories of data subjects,
  - Description of the categories of personal data,
  - Categories of recipients to whom the personal data is disclosed,
  - Transfers to third countries (if applicable),
  - Description of the technical & organisational security measures adopted.
- Personal data may only be transferred to another country if:
  - The EU has determined that the destination country has an adequate level of data protection,
  - The transfer is subject to contractual clauses approved by the EU,
  - It is required for fulfilment of Shorcontrol Safety's relevant business needs,
  - It is required for fulfilment of the data subject's needs.
- Shorcontrol Safety may engage certain service providers to perform certain services on its behalf which may involve the Processing of Personal Data e.g., Third parties that assist with the distribution of Shorcontrol Safety newsletters and emails.
- To the extent that such processing is undertaken based on the instructions of Shorcontrol Safety and gives rise to a Data Controller and Data Processor relationship, we will ensure that such relationships are governed by a contract which includes the data protections prescribed by Data Protection Law.

5.4 Individual Data Subject Rights

Data Protection Law provides certain rights in favour of data subject. The rights in question are as follows:

- The right of a data subject to receive detailed information on the processing (by the virtue of the transparency obligations on the Controller),
- The right of access to Personal Data,
- The right to rectify or erase Personal Data (right to be forgotten),
- The right to restrict processing,
- The right of data portability,
- The right of objection,
- The right to object to automated decision making, including profiling, and where CMC relies on its legitimate interests to Process data.
- These Data Subject Rights will be exercisable by individuals subject to limitation as provided for under Data Protection Law. Individuals may make a request to exercise any of the Data Subject Rights by contacting Shorcontrol Safety at privacy@safety.ie

5.5 Accuracy of Information Retained

- It is assumed that in the absence of evidence to the contrary, the information provided to Shorcontrol Safety is deemed accurate.

- If Shorcontrol Safety becomes informed or aware of any inaccuracies in the information retained, that information shall be promptly rectified by the company.
- Shorcontrol Safety does not retain any information about individuals that is either out of date or no longer required.

5.6 Information Used for Training Purposes

- Shorcontrol Safety will only collect and retain information required to process an individual's interaction with and through the company.
- Such information will be used and relayed to Accredited Governing Bodies whom Shorcontrol Safety has an agreement with to provided training on behalf of.
- The information relayed and used with the Accredited Governing Bodies will be limited to only pertinent information which is required in order to register and/or acquire an individual's certificate, diploma, or otherwise award received for participation and/or successful completion and passing of a training program.

5.7 Blended Learning and Live-Remote Information Use and Retention

- Shorcontrol Safety will only share pertinent and required information, related to individuals, to tutors who are administrating blended learning and/or live-remote training.
- Information supplied and used for blended learning and live-remote training courses will be able to be used to identify individuals while they participate in the course.
- The use of identifying information is necessary to use in order to ensure that the integrity of the program is kept in-tact, that the individual who is registered for the course is the same individual who is attending the course, and to ensure that no cheating, plagiarism, or otherwise foul play is committed during the administration of the course.

5.8 Types of Information Collected from Visitors to the Company Website

- Only non-personal data is collected from visitors to the website.
- Shorcontrol Safety collects statistical and other analytical information on an aggregate basis.
- The information collected cannot be used to identify or contact individuals.
- Demographic information collected pertains to browser types and other anonymous statistical data involving use of the site.
- The collection of non-personal data is used to gain a better understanding of where individuals are coming from and to better aid in the design and organisation of the website.
- The Shorcontrol Safety website utilises web browser cookies which included use of an anonymous unique identifier.
- Visitors to the site will be asked permission to store cookies onto the individuals personal web browser.
- Individuals can opt out of allowing cookies while still being able to use the site.
- The Shorcontrol Safety website designs and uses its cookies to give individuals the best possible experience when visiting the site.
- The Shorcontrol Safety website only uses cookies for which it has explicitly asked to use and store on an individual's personal web browser.
- Third party cookies are set on behalf of Safety.ie. These partner cookies do not collect personal data and would not be able to identify individual users.
- Cookies are used for the following:
    - For technical purposes essential to the effective operation of the website.
    - To enable Safety.ie to collect anonymous information about the browsing activities of our clients for internal analysis.
    - To drive Safety.ie marketing activities.
- Any changes made to this policy will be posted on Safety.ie.

5.9 Breach of Data Integrity

5.9.1 Suspicion of Data breach

A data breach may not be apparent when it initially occurs. Therefore, the following steps shall be followed to determine whether a credible data breach has occurred or not.

- If a data breach is suspected, an investigation must be initiated to determine what information has been stolen, lost, or otherwise compromised.
- At Shorcontrol Safety we use 'Itomic'; an information technology (IT) company to manage all IT related needs. Itomic shall be notified of suspect data breach and are required to assist in the investigation.
- All employees shall be requested to review their business email accounts and search for;
    - Suspicious emails that have either been sent or received to/from their account.
    - Suspicious email addresses that they do not recognise and are found in their contact lists.
    - Suspicious emails sent or received to/from their account outside their regular hours of work e.g., late night, weekends, holidays etc.
- Data which is suspect of being compromised shall be cross checked with hard copies (if available). This is to ensure that data has not been altered while also aiding in the discovery of any removal or destruction of digital copies.
- Where possible, missing copies must be replaced using existing copies sourced from other locations e.g., clients.

5.9.2 Confirmation of Data breach

Following the initial investigation, if a data breach has occurred then the following steps must be taken:

- The Data Protection Commission must be notified with the below details within 72 hours, if the breach consists of a natural person's personal data concerns their racial of ethnic origin, political opinion, religious or philosophical beliefs, sexuality or sexual orientation, trade union membership, health or genetic data, criminal convictions, identification documents or financial data:
    - Type of breach, confidentiality, availability and/or integrity of breach,
    - Nature, sensitivity, and volume of data,
    - Severity of potential consequences for affected individuals,
    - Ease of identification of affected individuals,
    - Contact information for Shorcontrol Safety's personnel who are tasked with overseeing the investigation,
    - Measures that Shorcontrol Safety have taken or propose to take, to address the breach and reduce the likelihood of a similar breach occurring in the future.
- If the natural persons personal data consists of the following only then the Data Protection Commission does not need to be made aware of the breach:
    - Data that is publicly available
    - Data that is encrypted with state-of-the-art algorithm, securely hashed, and salted, and the key remains confidential and cannot be independently ascertained.
    - There is a very temporary loss of access to personal data.
    - The data was accidently sent to a third party, who can be trusted by virtue of their relationship with Shorcontrol Safety to comply with instructions to relay the extent of the data sent to them, destroy the data, and prevent further release of data beyond their control.
- If the data breach is of the nature which requires the Data Protection Commission be notified, then the affected individuals must be notified of the following details:
    - Contact details of the Shorcontrol Safety person who is tasked with overseeing the investigation and/or communication to the affected persons.
    - A description of the extent and nature of the breach.
    - Potential consequences of the breach.
    - Measures that Shorcontrol Safety have taken or propose to take to address the breach.

  - Advice on how the affected persons can protect themselves from potential consequences of the breach.
- Whether the Data Protection Commission needs to be made aware of the data breach or not, all affected persons/clients of any breach must be notified of the following details:
  - Contact details of Shorcontrol Safety's person who is tasked with overseeing the investigation and/or communication to affected individuals.
  - A description of the extent and nature of the breach.
  - Measures that Shorcontrol Safety have taken or propose to take to address the breach.

5.9.3 Documentation and Further Investigation

- Documentation and recording of data breaches must be recorded in order to comply with the GDPR. This includes:
  - The report given to the Data Protection Commission.
  - All communication between Shorcontrol Safety, Itomic, DPC and affected individuals.
  - Steps taken to mitigate the data breach.
  - Steps or decisions made by Shorcontrol Safety to reduce the likelihood of another breach occurring in the future.
- If there are new discoveries related to the initial data breach, then Shorcontrol Safety must:
  - Notify the DPC of any updates.
  - Notify affected individuals, only if the discoveries differ from the initial notification.
  - Notify newly discovered affected individuals.

5.10 Data Destruction

This section is to ensure secure, lawful, and traceable destruction of client data upon request or when no longer required.

- Legal Compliance:
  - Follows GDPR and Data Protection Act 2018.
  - Supports ISO 45001 risk management principles.
- When Data Is Destroyed:
  - Upon client request.
  - After retention periods expire.
  - When data is no longer needed.
  - If consent is withdrawn.
  - At contract termination.
- Destruction Methods:
  - Electronic: Secure erasure software, degaussing, cryptographic wipe.
  - Physical: Shredding, crushing, or certified incineration.
  - Proof: Certificates of destruction must be issued and logged.
- Documentation:
  - Maintain a Data Destruction Log with:
    - Type of data
    - Method used
    - Date/time
    - Responsible staff
- Roles & Responsibilities:
  - DPO: Oversees compliance.
  - IT: Executes secure deletion.
  - Managers: Ensure proper classification.
  - Staff: Follow procedures and report issues.

- Client Communication:
  - Inform clients of:
    - Their rights
    - Retention periods
    - Destruction procedures
    - Any associated costs

5.11 Data Encryption

This section is to ensure all sensitive data—whether at rest, in transit, or in use—is protected through appropriate encryption methods, reducing the risk of unauthorised access or data breaches. IT applies to all employees and contractors or third-party service providers who handle or access the organisations data systems or communications.

Data in Transit

- All data transmitted over public or unsecured networks must be encrypted using TLS 1.2 or higher.
- Email communications containing sensitive information must use end-to-end encryption or secure portals.

Data at Rest

- Sensitive data stored on servers, databases, laptops, and mobile devices must be encrypted using AES-256 or equivalent.
- Encryption keys must be stored securely and separately from the encrypted data.

Portable Media

- USB drives, external hard drives, and other portable media must be encrypted before storing any company or client data.
- Use of portable media must be approved by IT and logged.

Cloud Services

- Cloud providers must support encryption for both data at rest and in transit.
- Contracts must include clauses ensuring encryption standards and key management practices.

Key Management

Encryption keys must be:

- Generated securely
- Stored in a secure key vault
- Rotated periodically
- Accessed only by authorized personnel

Mobile Devices

- Company-issued mobile devices must use full-disk encryption.
- Personal devices used for work must comply with mobile device management (MDM) policies.

5.12 Additional Information

- If at any time the company decides to use Personal Data in a manner significantly different from that stated in this policy or otherwise disclosed to the individual at the time of its collection, Shorcontrol Safety will notify the individual by email, and the individual will have a choice as to whether or not allow its information to be used in the new manner.

- In the cases of a personal data breach likely to result in a risk to the rights and freedoms of a natural person, the processor shall notify the controller as soon as they are aware of the breach.

- The controller shall within 72 hours after becoming aware of the breach, notify the relevant EU supervisor authority.
- The controller shall also communicate the breach, in clear and plain language to any data subject affected by the breach.

6. Responsibilities

Employee Title/Classification	Responsibility
Directors, Top Management & Senior Management	To ensure the necessary resources are available within the organisation for the implementation of this policy. To ensure the contents of this policy are implemented effectively. To investigate and act upon any breaches or violations which may arise or be reported in relation to this policy.
Employees/ Staff/ Instructors/ Sub-contractors	To adhere to the requirements set out in this policy. To report any breaches or violation of this policy to top/senior management for investigation and resolution.

7. Enforcement

Employee Title/Classification	Responsibility
General Manager	Has the discretion of determining the repercussion on the discovery of any member of staff, tutors, managers, visitors, or subcontractor's breach or violation of this policy. Has the discretion of determining the repercussions on the discovery of a manager or assigned responsible personnel's failure to enforce or follow this policy or its procedures.
Managers and Heads of Departments	Has the discretion of determining the repercussions on the discovery of any subordinate or learner's breach or violation of this policy.

8. Related Information and Documents

Document ID	Title
External Information	• Overview of the General Data Protection Regulation (GDPR) (citizensinformation.ie) • How to access your personal data under the GDPR (citizensinformation.ie) • Controlling and processing personal data (citizensinformation.ie) • Data Protection Act 2018 (irishstatutebook.ie) • Homepage | Data Protection Commission • https://forms.dataprotection.ie/report-a-breach-of-personal-data
OCC-PRO-003	Data Breach & Integrity Procedure – Occupational Hygiene
Core Communications	www.corecom.ie
Innotech	www.innotech.ie

9. Policy Review

This policy shall be reviewed when:

- There is a change in law and legislation (GDPR or otherwise).
- There is a change of General Manager at Shorcontrol Safety.
- There is a change in any of the related policies or procedures found in section 8. *'Related Information & Documentation'* of this document.
- As prescribed in Shorcontrol Safety's policy and procedure review schedule.
- As determined or requested by the General Manager at Shorcontrol Safety.

Revision Date	Author with Title	Description
	John Kelly; Head of Training & Development	Review and update of previous version.
	Adam Romans; Quality Coordinator	Review, update, and format standardisation.
20/02/2023	Angela Byrne; QHSM	Review, update and reformat layout/structure. Inclusion of Data Breach Integrity from GEN-PRO-008.
08/03/2024	Angela Byrne; QHSM	Review – no change.
27/05/2025	Angela Byrne; QHSM	Review – removal of Itomic as is no longer used as external communications provider. Occ. Hygiene procedure, Innotech and Core Communications added to section 8.
26/07/2025	Angela Byrne; QHSM	Inclusion of data encryption in section 5.