Data Protection and ISMS Policy

1. Introduction

Most businesses hold personal data on their clients, employees and partners. The explosion in the use of the Internet, electronic communication and computerisation of business data has led to an increase in the importance of privacy. Breaches of computerised data security have prompted the introduction of legislation on a national and European level. These include:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000
- Data Protection Act 2018
- Computer Misuse Act 1990
- European Union General Data Protection Regulation (EU GDPR)

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the “rights and freedoms” of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Senior Management of IISACCS are strongly committed to the rights of individuals whose data they collect and process and will comply with UK and EU laws related to personal information in- line with the EU General Data Protection Regulation (GDPR).

To achieve this, Senior Management of IISACCS has implemented a Personal Information Management System (PIMS) which is maintained and improved continuously.

The PIMS, that Senior Management of IISACCS has implemented meets its requirements under the EU GDPR for the management of personal information and will be continuously maintained and improved. The PIMS ensures that the objectives of IISACCS and obligations under the law are met and it ensures that controls are in place that reflects the level of risk that IISACCS is willing to accept. In addition, the PIMS ensures that IISACCS is able to meet all the regulatory, statutory and contractual obligations that are applicable. Most importantly the PIMS enables IISACCS to protect the interests of individuals and all other relevant stakeholders.

To comply with the requirements of GDPR, IISACCS will:

- Process personal information only where this is strictly necessary for legitimate organisational purposes
- Collect only the minimum personal information required for these purposes and not process excessive amounts of personal information
- Provide clear information to individuals about how their personal information will be used and who will be using the information
- Only process relevant and adequate personal information
- Process personal information fairly and lawfully

- Keep all personal information secure
- Maintain an inventory of the categories of personal information that is processed
- Ensure they keep personal information accurate and up to date
- Retain personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes
- Respect individuals' rights in relation to their personal information as defined in the GDPR.
- Only transfer personal information outside the EU Member States in circumstances where it can be adequately protected and aligned with EU GDPR Regulations
- Only apply exemptions permitted by data protection legislation;
- Develop and implement a PIMS to enable the policy to be implemented
- Identify internal and external stakeholders and the degree to which these stakeholders are involved in the governance of IISACCS' PIMS
- Identify staff with specific responsibility and accountability for the ongoing maintenance and support of the PIMS.

2. Notification to the Information Commissioners Office (ICO)

IISACCS has notified the Information Commissioner that it is a data controller and that it processes personal data. IISACCS has identified and recorded all the personal data that it processes in the Data Register.

A record of notification to the ICO is retained by the Data Protection Officer in our database system and the ICO Notification Handbook is used as the authoritative guidance for notification. This notification is reviewed annually and update notifications issued accordingly.

The Data Protection Officer is responsible for reviewing the details of notification to ensure that any changes to the way IISACCS processes or controls personal data (as determined by changes to the Data Register and following management review) are referred back to the ICO. Additional requirements for notification may also arise from Personal Data Impact Assessments.

This policy applies to all employees and processors of IISACCS such as outsourced suppliers. Any breach of the GDPR or this PIMS will be considered as a breach of the disciplinary policy and could also be considered a criminal offence, potentially resulting in prosecution.

All third parties working with or for IISACCS, and who have or may have access to personal information, will be expected to comply with this policy. All third parties who require access to personal data will be required to sign a non-disclosure agreement before access is permitted. This agreement will ensure that the third party has the same legal obligations as IISACCS. This will also include an agreement that IISACCS can audit compliance with the agreement.

GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services or monitor the behaviour of data subjects who reside in the EU.

Data Protection and ISMS Policy

3. Key Definitions

Personal data – this is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Data Protection and ISMS Policy

4. Scope of Information

In order to be able to carry out its legal requirements, IISACCS is required to collect certain data from its clients. Carrying out Retrofit Designs on eligible properties is subject to the company successfully reviewing specific property information. In such instances, IISACCS is provided with personal data from its clients' customers in order to ensure the success of its application. Data is processed on the following basis:

a) The data subject has given consent to the processing of their personal data for one or more specific purposes;
b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) Processing is necessary for compliance with a legal obligation to which the controller is subject.

IISACCS recognises that its records are an important asset and they are available to those who are entitled to see them. They are a key resource for the effective operation and accountability of the company. Like any other asset, they require careful management and this policy sets out the company's responsibilities and activities for the management of its records. We may receive the following information from clients with regards to their direct customers:

- Name
- Contact information including email address
- Demographic information
- Website usage data
- Other information relevant to client enquiries
- Other information pertaining to special offers and surveys.

5. Purpose of Data Collection

Collecting this data helps us with our continuous improvement and enables us to deliver our services. Specifically, we may use data:

- For our own internal records.
- To improve the products and services we provide.
- To contact you in response to a specific enquiry.
- To customise the website for you.
- To send you promotional emails about products, services, offers and other things we think might be relevant to you only in the cases where if appropriate consent was given.

6. Risk Assessment in relation to GDPR

IISACCS has assessed the risks associated with the processing of all types of personal information. A Risk Assessment procedure has been implemented and is used by the company to monitor any risk to individuals during processing of their personal information. Assessments will also be completed by IISACCS for any processing that is undertaken on their behalf by any third-party organisation IISACCS will also, through the application of the Risk Assessment procedure, ensure that any identified risks are managed appropriately to reduce the risk of non-compliance.

6. Risk Assessment in relation to GDPR Cont.

Data Protection and ISMS Policy

Where processing of personal information may result in a high risk to the “rights and freedoms” of natural persons, IISACCS shall complete a data protection impact assessment, prior to conducting the processing, to ensure the personal information is protected. This assessment may also be used to apply to a number of similar processing scenarios with a similar level of risk.

Where, as a result of a Data Protection Impact Assessment, it is clear that IISACCS will process personal information in a manner that may cause damage and/or distress to the data subjects, the DPO will review the process before IISACCS proceeds to process the information. If the Data Protection Officer decides that there are significant risks to the data subject, they will seek the ICO for final guidance.

7. Principles of Data Protection

Any processing of personal data must be conducted in accordance with the following data protection principles of the Regulation and IISACCS policies and procedures within the PIMS will ensure compliance.

Personal data must be processed lawfully, fairly and transparently. IISACCS’ Fair Processing Procedure (PIMS PR03 Fair Processing Procedure) details how this is achieved. The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals’ “rights and freedoms”. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must as a minimum include:

- The identity and the contact details of the data controller and, if any, of the data controller's representative;
- The contact details of the Data Protection Officer, where applicable;
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- The period for which the personal data will be stored;
- The existence of the rights to request access, rectification, erasure or to object to the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients of the personal data, where applicable;
- Where applicable, that the data controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- Any further information necessary to guarantee fair processing.

Personal data can only be collected for specified, explicit and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of IISACCS’ GDPR registration. (PIMS PR03 Fair Processing Procedure)

Personal data must be adequate, relevant and limited to what is necessary for processing. The Data Protection Officer is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

7. Principles of Data Protection Cont.

All data collection methods (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Data Protection Officer and approval recorded.

The Data Protection Officer will ensure that all data collection methods are reviewed annually by internal audit or external experts to ensure that collection continues to be adequate, relevant and not excessive.

The Data Protection Officer is responsible for ensuring that any data that is shown to have been obtained excessively, or is not specifically required by IISACCS, is securely deleted or destroyed in line with the Data Protection & Storage Media Procedure.

8. Other Considerations

Personal data must be accurate and kept up to date.

Data that is kept for a long time must be reviewed and updated as necessary. Any data that is considered to be inaccurate or likely to be inaccurate must be removed.

Senior Management is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

All individuals are responsible for ensuring that any data held by IISACCS is accurate and up-to-date. Any data submitted by an individual to a company, such as via a registration form, will be considered to be accurate at the time of receipt.

Employees or other individuals should notify IISACCS of any changes in personal information to ensure personal information is kept up to date (Instructions for updating records are contained in the HR34 Change of Personal Detail Form). It is the responsibility of IISACCS to ensure that any notification of changes to personal information is implemented.

The Data Protection Officer is responsible for ensuring that all necessary actions are taken to ensure personal information is accurate and up to date. This should also take into account the volume of data collected, the speed with which it might change and any other relevant factors.

The Data Protection Officer will review, at least once a year, all the personal data processed by IISACCS, held in the Data Register. The Data Protection Officer will note any data that is no longer required in the context of the registered purpose and will ensure that it is appropriately removed and securely disposed of in line with the Data Protection & Storage Media Handling Procedure.

If a third-party organisation has provided inaccurate or out-of-date personal information, the Data Protection Officer is responsible for informing them that the personal information is inaccurate and/or out-of-date and advise them that the information should no longer be used. The Data Protection Officer should also ensure that any correction to the personal information is passed on to the third party.

9. Personal Data Considerations

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing. Where personal data is retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach.

9. Personal Data Considerations Cont.

Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure (PIMS PR05 Retention of Records Procedure).

The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in the Retention of Records procedure, (PIMS PR05 Retention of Records Procedure), and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

Personal data must be processed in a manner that ensures its security. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to audit and review.

IISACCS' compliance with this principle is contained in its Information Security Management System (ISMS).

10. Accountability

The GDPR states that the data controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR. As a result, controllers are required to keep all necessary documentation of all processing operations, and implement appropriate security measures. They are also responsible for completing Data Processing Impact Assessments (DPIAs), complying with requirements for prior notifications, or approval from supervisory authorities and ensuring a Data Protection Officer is appointed if required.

11. Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO to assess whether any provision of the GDPR has been contravened.
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- The right to object to any automated profiling without consent.

11. Data subjects' rights Cont.

Data subjects may make data access requests as described in the Subject Access Requests procedure, (PIMS F04 Subject Access Requests Form). This procedure also describes how IISACCS will ensure that its response to the data access request complies with the requirements of the Regulation.

12. Complaints

A Data Subject has the right to complain to at any time to IISACCS if they have concerns about how their information is used. If they wish to lodge a complaint this should be directed to the DPO following the complaints procedure using a complaint form supplied by IISACCS. In addition, a Fair Processing Notice (PIMS F03) will be provided.

A Data subject also has the option to complain directly to the Information Commissioners Office via their website: https://ico.org.uk/

13. Consent

IISACCS understands 'consent' as the explicit and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

In addition, IISACCS understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent (PIMS F01 Customer Consent Form) of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Consent to process personal and sensitive data is obtained routinely by IISACCS using standard consent documents (PIMS PR01 Consent Procedure). This may be through a contract of employment or during induction.

Where IISACCS provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit – which may be no lower than 13.

14. Data Security

All IISACCS employees that are responsible for any personal data which IISACCS holds must keep it secure and ensure that it is not disclosed under any conditions to any third party. A third party can be authorised by IISACCS to receive that information however it must accept and sign a confidentiality agreement (NDA).

All personal data will be accessible only to those who need to use it. Employees should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, it must be password protected in line with the Access Control Policy; stored on encrypted removable media in line with the Data Protection & Storage Media Handling Procedure.

Steps will be taken to ensure that PC screens and terminals are not visible except to authorised Staff of IISACCS. All staff must sign up to the Acceptable Use Policy before they are given access to organisational information of any sort.

Manual records will not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they will be removed from secure archiving.

Personal data may only be deleted or disposed of in line with the Retention of Records Procedure (PIMS PR05). Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by the Data Protection & Storage Media Handling Procedure before disposal. Because of the increased risk all Staff must be specifically authorised to process data off-site.

15. Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held IISACCS in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by IISACCS, and information obtained from third-party organisations about that person. Subject Access Requests are dealt with as described in PIMS PR04 Subject Access Request Procedure.

16. Disclosure of data

IISACCS will ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees must exercise caution when asked to disclose personal data held on another individual to a third party (and will be required to attend specific training that enables them to deal effectively with any such risk). It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of IISACCS' business.

GDPR permits a number of exemptions where certain disclosure without consent is permitted, as long as the information is requested for one or more of the following purposes:

- To safeguard national security;
- To prevent or detect crime including the apprehension or prosecution of offenders;
- To assess or collect tax duty;
- Discharge of regulatory functions (includes health, safety and welfare of persons at work);
- To prevent serious harm to a third party;
- To protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

17. Retention and disposal of data

Personal data may not be retained for longer than it is required. Once an employee has ended their employment with IISACCS, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. IISACCS' data retention and data disposal procedures (PIMS06. Retention of Records & the Data Protection & Storage Media Handling Procedure) will apply in all cases.

18. Disposal of records

Personal data will be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal procedure.

Please refer to P025 for Secure Disposal of IT Equipment and Information.

19. E-mail and Internet privacy

Data Protection and ISMS Policy

The inappropriate use of e-mail and the Internet by employees, e.g. using the Internet for non-work purposes, can have significant consequences for the organisation. This can be in terms of:

- Embarrassment/damage to IISACCS' reputation
- Loss of productivity
- Increased risk of liability and legal action, e.g. for sexist or racist e-mails
- Increased virus risk

To avoid inappropriate usage, we have introduced security electronic safeguards. A firewall checks, guarantees and manages e-mail attachments. The Organisation has installed filtering software that searches e-mails for specific words or phrases, normally obscene or discriminatory, and monitors which websites our employees are accessing as well as filtering which types of websites our employees can access.

Please see the E-mail & Internet Usage and Social Media Policy. In addition, IISACCS employees will be kept fully informed about overall information security procedures and the importance of their role within these procedures. Similarly, manual filing systems are held in secure locations and only authorised employees can access them.

20. Company Responsibilities

As with other considerations including Quality and Health & Safety, Information Security aspects are taken into account in all daily activities, processes, plans, projects, contracts and partnerships entered into by the Organisation. The following are IISACCS other responsibilities in relation of ISMS:

- Employees are trained on general and specific aspects of Information Security, according to the requirements of their function within the Organisation;
- Communication of the disciplinary actions taken from breaching the Information Security policies and procedures by the IISACCS employees;
- In view of the IISACCS position as a trusted provider of providing compliant Retrofit advice and designs, particular care is taken in all procedures and by all employees to safeguard the Information Security of its service users and/or clients. When relevant, agreements of Mutual Non-disclosure/Confidentiality are entered into as appropriate with third party Companies;
- All statutory and regulatory requirements are met and regularly monitored for changes;
- A Business Continuity Plan is maintained, tested and subjected to regular review by the ISMS Manager;
- Further policies and procedures such as those for access, acceptable use of e-mail and the Internet, virus protection, backups, passwords, systems monitoring etc. are in place, maintained and are regularly reviewed by the ISMS Manager or an appointed representative, as appropriate;
- This Information Security Policy is regularly reviewed and may be amended by the Managing Director in order to ensure its continuing viability, applicability and legal compliance, and with a view to achieving continual improvement in the Information Security Systems.

21. Other Responsibilities

IISACCS is a data controller and data processor as defined under the GDPR.

Senior Management and all those in managerial or supervisory roles throughout IISACCS are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.

Data Protection and ISMS Policy

ISMS Manager – Overall responsibility for Information Security rests with the ISMS Manager, which includes:

- The day-to-day responsibility for procedural matters, legal compliance, maintenance and updating of documentation;
- Promotion of security awareness, liaison with external organisations, incident investigation and management reporting etc;
- Technical matters i.e. technical documentation, systems monitoring, technical incident investigation and liaison with technical contacts at external organisations;
- Drafting, maintaining and implementing this Security Policy and similarly related documents.

All employees – duty to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security without delay, direct to the ISMS Manager. Employees attending external sites must ensure the security of the Organisation's data and access their systems by taking particular care of laptop and similar devices and of any information on paper or other media that they have in their possession. Employees must ensure adherence to Information Security procedures as set out in IISACCS' various policies and guideline documents as part of all employees' contractual duty as set out in the Contracts of Employment.

Data Protection Officer – accountable to the Senior Management of IISACCS for the management of personal information by IISACCS and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes the development and implementation of the Information Security Management System to ensure compliance.

IISACCS has appointed a member of the management team to act as the Data Protection Officer (DPO) who is responsible for the organisations compliance with this policy. The DPO is responsible for ensuring that IISACCS complies with the GDPR in relation to all aspects of data processing. The DPO has direct responsibility for policy and procedures, including Subject Access Requests. The DPO is also the person to whom all staff will go to seek guidance regarding GDPR compliance.

It should be noted that compliance with Data Protection and GDPR requirements remains the responsibility of all staff who process or control personal information for IISACCS. All employees employed by IISACCS are also responsible for ensuring that any personal data that is about them that is supplied by them to IISACCS is accurate and up-to-date.

22. Review

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the EU General Data Protection Regulation.

The Data Protection Policy will, under normal circumstances, be managed and reviewed annually. The reviews to the Policy will be subject to scrutiny and, from time to time, updates and re-issues will be circulated.

However, the Policy will be reviewed sooner in the event of any one or more of the following:

- Weaknesses in the Policy are highlighted; or
- Weaknesses in hardware and software controls are identified; or
- In case of new threat(s) or changed risks; or
- Changes in legislative requirements; or
- Changes in Government, company or other directives and requirements.

Data Protection and ISMS Policy

Introduction

IISACCS Information Security Policy applies to all business functions within the scope of the Information Security Management System and covers the information, information systems, networks, physical environment and people supporting these business functions. This document states the Information Security objectives and summarises the main points of the Information Security Policy.

In order to operate IISACCS require certain types of information from our employees, clients and other individuals. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this is within the Data Protection Act 2018 and EU General Data Protection Regulation (GDPR).

Objective

The objective of Information Security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. In particular, information assets must be protected in order to ensure:

1. Confidentiality i.e. protection against unauthorised disclosure
2. Integrity i.e. protection against unauthorised or accidental modification
3. Availability as and when required in pursuance of the Organisation's business objectives.

Employees, verified subcontractors and clients of IISACCS are required to understand the purpose and principles of the GDPR and to follow the guidelines and procedures in place. Failure to adhere to the Data Protection Act 2018 and EU General Data Protection Regulation could result in legal action.

Principles

Data users must comply with the data protection principles of good practice, which underpin the Act. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this IISACCS follows the six Data Protection Principles outlined in the Data Protection Act 2018 and GDPR, which are summarised below:

1. Lawfulness, fairness and transparency
2. Purpose limitations
3. Data minimisation
4. Data Accuracy
5. Data Retention
6. Integrity and confidentiality

IISACCS employees who process or use any personal information in the course of their duties will ensure that these principles are followed at all times.

Signed: *a beaumont*

Position: Managing Director

Date: 19/07/2025

Revision: 00