The Institute of Customer Service

Data Protection Policy

1. Introduction

The Institute collects and uses information about people with whom it works including employees, members, their customers and suppliers. Personal data must be handled and dealt with properly, regardless of how it is collected, recorded and used. The Institute will ensure that it treats personal information lawfully and correctly.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to undertake a Privacy Impact Assessment (PIA) and ensure that The Institute Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Personal data means information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, customers, suppliers and marketing contacts.

2. Scope

This policy applies to all staff. You must ensure you read this policy and understand what it means in practice for you in your role. This policy supplements our other policies relating to IT, internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time.

3. Who is responsible for this policy?

As our Data Protection Officer, the CFO Bill Leonard has overall responsibility for the day-to-day implementation of this policy. The Data Protection Officer's responsibilities are:

a. Keeping the board updated about data protection responsibilities, risks and issues

b. Reviewing all data protection procedures and policies on a regular basis

c. Ensuring that HR arrange data protection training and advice for all staff members and those covered by this policy

d. Answering questions on data protection from staff, board members and other stakeholders

e. Responding to individuals such as clients and employees who wish to know which data is being held on them by The Institute.

f. Ensuring that contracts with third parties that handle personal data on behalf of The Institute are approved by the CFO.

The responsibilities of the Head of Operations are:

a. Ensuring all systems, services, software and equipment meet acceptable security standards

b. Checking and scanning security hardware and software regularly to ensure it is functioning properly

c. Researching third-party services, such as cloud services the company is considering using to store or process data

The responsibilities of the Director of Communications and Corporate Affairs are:

a. Approving data protection statements attached to emails and other marketing copy

b. Addressing data protection queries from clients, target audiences or media outlets

c. Coordinating with the Data Protection Officer to ensure all marketing initiatives adhere to data protection laws and the Data Protection Policy

4. Personal Data Management

The Institute will protect Personal Data gathered and used in the course of conducting business activity via a range of activities including (as appropriate):

- specifying the purpose for which information gathered is used

- gaining consent (where necessary) for the collection and processing of personal data
- collecting and processing appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- taking steps to ensure the quality of information used
- applying a rationale to establish the length of time information is held
- taking appropriate technical and organisational security measures to safeguard personal information
- ensuring that personal information is not transferred abroad without suitable safeguards
- setting out clear procedures for responding to requests for information.
- ensuring that the rights of people about whom the information is held can be fully exercised under the Regulation/Act including the right to:
    - be informed that processing is being undertaken;
    - access to personal information within the statutory 30 days;
    - prevent processing in certain circumstances;
    - correct, rectify, block or erase information.

In addition, The Institute will ensure that:

- everyone managing and handling personal information is trained and understands that they are contractually responsible for following good data protection practice and that breach of this policy could constitute a breach of contractual terms;
- anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;

- queries about handling personal information are dealt with promptly and courteously;
- methods and performance in the handling of personal information are regularly assessed and evaluated.

The Institute will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that paper files and other records or documents containing personal/sensitive data are kept in a secure environment, and personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically. (Individual passwords are such that they are not easily compromised).

4. Processing

The processing of all personal data must be:

a. Necessary to deliver our services or comply with a legal requirement.

b. In our legitimate interests and not unduly prejudice any individual's privacy.

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects via The Institute Privacy Notice.

5. Sensitive personal data

In most cases where we process sensitive personal data (e.g. HR collection of demographic data such as diversity data) we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations). Any such consent will clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

6. Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Data Protection Officer.

7. Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. So if your personal circumstances change, affecting the personal data we hold about you please contact (depending on what data it is) The Institute Data Protection Officer, Head of HR or Head of Operations so that it can be corrected.

8. Data security

Institute employees are required to keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Data Protection Officer will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

a. In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it

b. Printed data should be shredded when it is no longer needed

c. Data stored on memory sticks must be locked away securely when they are not being used

d. The Head of Operations must approve any cloud used to store data

e. Servers containing personal data must be kept in a secure location, away from general office space

f. Data should be regularly backed up in line with The Institute's backup procedures

g. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

h. All servers containing sensitive data must be approved and protected by security software and strong firewall.

9. Data retention

We must not keep personal data for longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

10. Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Institute Data Protection Officer and/or Head of Operations. Please refer to The Institute **Extra EEA data transfer policy** and ensure you understand the content.

11. Subject access requests (SARs)

Individuals are entitled, subject to certain exceptions, to request access to personal data held by The Institute about them. These requests are called Subject Access Requests and will be processed within 30 days maximum.

If you receive a subject access request from a member or other customer, you should apply the **Subject Access Policy** and ensure the Data Protection Officer is informed (by email).

If you wish to request or correct information that The Institute holds about you, you must apply using the internal SAR policy and form. There are restrictions on the information to which you are entitled under applicable law.

12. Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Data Protection Officer about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them and consent for you to contact them in relation to the services being marketed.

Please contact the Director of Communications and Corporate Affairs/Data Protection Officer for advice on direct marketing before starting any new direct marketing activity.

13. Training

All staff receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure. Training will cover:

- The law relating to data protection
- Our data protection and related policies and procedures including privacy impact assessments

Completion of training is compulsory.

14. Privacy Notice

The Institute Privacy Notice:

a. Sets out the purposes for which we hold personal data

b. Highlights that our work may require us to give information to third parties

c. Provides that customers have a right of access to the personal data that we hold about them

The privacy notice may be downloaded from the website.

Being transparent and providing accessible information to individuals about how we will use their personal data is important for The Institute and its customers.

15. Consent

Where we gather data with the consent of the data subject, that consent must be current and active. The Institute does not use pre-ticked consent boxes and silence is not presumed to be consent. Consent can be revoked at any time – and where this occurs the individual will (in most cases) have the right to have their personal data deleted.

16. Right to be forgotten

A data subject may request that information held on them by The Institute is deleted or removed and where applicable, third parties who process or use that data must also comply with the request. An erasure request can only be refused if one of the following applies:

a) In the exercise of the right to freedom of expression and information.

b) Compliances with a legal obligation or public interest task.

c) Public health or archiving purposes in the public interest.

d) In the exercise or defense of legal claims.

17. Privacy by design and default

Privacy by design is an approach to projects which promotes and protects privacy and data protection compliance from the start. Project owners are responsible for conducting Privacy Impact Assessments and ensuring the results are recorded both centrally and on relevant DT papers in the appropriate section, please see the **DT paper template** for further information.

The Privacy Impact Assessment Policy and screening form can be found **here.**

The Head of Operations is responsible for ensuring that all IT projects include a privacy impact assessment.

18. Data audit and register

Regular data audits to manage and mitigate risks will inform the **data risk register**. Audits contain information about what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

19. Reporting breaches

All members of staff have an obligation to read and understand The **Institute Data Breach policy** which sets out how to identify and report actual or potential data protection compliance failures. This allows The Institute to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Employees must report any suspected or actual data security breaches. This requirement applies regardless of whether the breach is accidental or otherwise. Data security breaches should be reported to the Head of Operations **David.Leen@icsmail.co.uk** for central logging and action.

20. Monitoring

Everyone must observe this policy. The Data Protection Officer has overall responsibility for this policy. It will be monitored regularly to ensure it is being adhered to. Compliance with this policy is very important. Failure to comply puts both you and The Institute at risk and therefore failure to comply with it may lead to disciplinary action.

21. Disclosure

The Institute may share personal data with other organisations such as partners, suppliers and other agencies only with the consent of the data subject. However there are some circumstances where the Institute may disclose personal data without the data subject's consent such as where The Institute is required to carry out a legal duty or protect the vital

interests of an individual or other person. Such disclosure is also permitted where the data subject has already made the information public.

22. Notification to the Information Commissioner

The Institute is registered as a data controller with the Information Commissioner's Office.

23. Change control information

Name of policy	Data Protection Policy v5.0
Version Number	5.0
Effective date	18/3/2016
Date of issue	21/3/2020
Date of next review	21/3/2021
Notable changes from previous version	Updated to reflect GDPR 2019 Updated to reflect contact email address of Head of Operations 2019
Policy owner	Data Protection Lead