Data Protection Policy
(ISO 27001:2013 Control A.18.1.4)

POLICY INFORMATION

Author	Corporate Data & Compliance
Policy reference	
Version	Final
Date of publication	December 2021
Aligned Standard	ISO 27001:2013 ISMS

APPROVAL AND OWNERSHIP

Department / Functional Ownership	Digital Directorate
Name of Owner	Corporate Data & Compliance
Approved By	Information and Data Approval Board (iDAB)

REVIEW HISTORY

Date of Last Review	January 2022
Date of Next Review	January 2023
Frequency of Review	Annually and on any substantial change

Contents

Reason for Policy

Scottish Water has a responsibility to protect the privacy of its people and customers and safeguard the valuable data and information entrusted to it.

Understanding this responsibility and adopting the correct behaviours and procedures when collecting and processing personal and business sensitive data and information helps ensure that Scottish Water meets its legal and regulatory obligations with the necessary controls in place.

This policy promotes good practice in data protection and observance of Data Protection Legislation by everyone who works for or carries out services on behalf of Scottish Water.

Scope

This policy applies to all personal and business sensitive data and information processed by or on behalf of Scottish Water.

It is applicable to all Scottish Water employees, contractors, service providers and any third parties collecting, accessing or using personal or business sensitive data or information processed by or on behalf of Scottish Water. It applies to personal or business sensitive data or information held on any digital assets, e.g. mobiles, laptops, removable devices, servers, applications, or hard copy in structured filing system.

Definition of the Policy

This policy defines Scottish Water's requirements relating to Data Protection.

Policy Details

1. Data Privacy & Protection Framework

Scottish Water will implement a Data Privacy & Protection Framework. The framework is overseen by Corporate Data and Compliance. The framework helps ensure that any changes to processes or technology that impact personal or business sensitive data and information, processed by or on behalf of Scottish Water, are risk assessed and comply with this policy.

A Privacy Impact Assessment is a compulsory requirement of the framework. The need for further documentation will be determined by Corporate Data and Compliance.

Details of activities where Scottish Water processes personal data will be recorded in a single inventory and for technological applications in an applications log maintained by Corporate Data and Compliance.

2. Classification, labelling and handling

Scottish Water will define its information classification, labelling and handling requirements in its Information Labelling and Handling Standard and Business Classification and Retention Scheme. The requirements apply to both personal and business sensitive information.

3. Personal Data Processing

Scottish Water will process personal data as follows. Personal data will be:

- Processed transparently and fairly
- Processed for specified, clear and lawful purposes
- Relevant and limited to the minimum needed to complete an activity
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Kept securely and accessed only by authorised persons
- Only shared with, or collected by a third party, where needed to enable a service to be provided on behalf of Scottish Water, where required by law, through the common duty of care to protect the life of an individual, or by consent of the individual

4. Personal Data Protection

To protect personal data Scottish Water will:

- Risk assess information containing personal data and handle it in accordance with the Information Labelling and Handling Standard and Business Classification and Retention Scheme
- Ensure appropriate levels of data and access controls are in place for personal data processed, by or on behalf of Scottish Water using technological applications
- Ensure compliance with the Test Data Policy when using data for technological application testing
- Fit all Scottish Water mobile IT equipment with contemporary cyber encryption and/or password controls
- Provide our people with appropriate training and raise awareness of data protection requirements

5. Personal Data - Individuals rights

Scottish Water will respect the rights of individuals as defined within relevant Data Protection Legislation.

Scottish Water will publish on its website and intranet details about an individual's rights, how to exercise those rights and how to complain.

Requests from individuals wishing to exercise their rights will only be considered and actioned by Corporate Data and Compliance. Scottish Water will verify the identity of any individual requesting personal data before they respond. Requests from a third party on behalf of an individual will only be actioned once the individual concerned has confirmed their agreement to release the information or data.

6. Personal Data - Transparency

Scottish Water will publish a privacy notice on its website and intranet outlining:

- How Scottish Water can be contacted about any personal data it holds
- Why Scottish Water collects and uses personal data
- How long Scottish Water will keep personal data
- How and when Scottish Water shares personal data with third parties
- If Scottish Water transfers any data outside of the EU

Functional Privacy Notices will also be completed. They will be made available on request through Corporate Data and Compliance.

7. Data Incidents

Scottish Water will have a Data Incident Response Plan in place to deal with any suspected personal or business sensitive data or information breach and to ensure that relevant Data Protection Legislation is complied with.

All data incidents must be reported as soon as they are identified to Corporate Data and Compliance.

8. Governance

The Scottish Water Data Protection Officer (DPO) will be a member of the Scottish Water Executive Leadership Team and is accountable to the Scottish Water Board of Directors for monitoring compliance with Data Protection Legislation and providing advice on data protection obligations within Scottish Water.

Mechanisms to monitor and support compliance with this policy will be introduced by Corporate Data and Compliance.

EXCEPTIONS

There are no exceptions to the contents of this policy.

VIOLATIONS

Failure to comply with this Policy may initiate the formal SW Disciplinary Policy and Procedures where potential sanctions may be up to and including dismissal. Appropriate measures may be put in place as deemed necessary such as restriction or withdrawal of access to SW information technology and communication facilities whilst the matter is fully investigated. Contractors, consultants or agency staff in breach of this policy may have their contract(s) terminated.

Terms and Definitions

Business Sensitive Data

Strategic, or operational information, of very high sensitivity where unauthorised disclosure or loss may have significant legal, regulatory, commercial, reputational or security repercussions.

Consent

An individual gives their agreement to process their personal data for a specific purpose. The agreement must be freely given, and evidenced by a statement or by a clear action taken by the individual.

Data Incident

An act or omission, either deliberate or in error, that compromises the security, confidentiality, integrity, or availability of personal or business sensitive data. A data incident becomes a data breach when it is confirmed that personal or business data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation, or if the data is made unavailable (for example, when it has been encrypted by ransomware, or accidentally lost or destroyed).

Data Protection Legislation

The Data Protection Act 2018 which embodies the requirements of the UK General Data Protection Regulations. Also any other relevant UK legislation, e.g.Privacy and Electronic Communications Regulations

Personal Data

Data, or information, that relates to a living person from which they can be identified.

Privacy Impact Assessment

A review to identify and reduce any risks associated with a data processing activity.

Privacy Notices

Notices that inform individuals how and why Scottish Water collects, processes, uses and shares personal data about them, and how Scottish Water keeps their data secure.

Processing

Collecting, using, storing, sharing personal data.

Related Documents

a. Information Labelling and Handling Standard
b. Business Classification & Retention Scheme
c. Data Incident Response Plan
d. Data Protection Standard
e. Information Management Policy
f. Access Management Policy