Data Protection Policy

POLICY INFORMATION

Author	Angela L. Jennings
Policy reference	CDC 002
Version	V 2.0
Date of publication	23.03.18

APPROVAL AND OWNERSHIP

Department / Functional Ownership	Corporate Data and Compliance
Name of Owner	Ingrid Severn, Head of Corporate Data and Compliance
Approved By	Data Protection Steering Group

REVIEW HISTORY

Date of Last Review	March 2018
Date of Next Review	March 2019
Frequency of Review	Annually or upon significant change

DOCUMENT HISTORY

Version	Date	Updated by	Reason for change
1.0	05.03.18	AJ	Initial Release
2.0	20.03.18	ITS	Final Approved Release

CONTENTS

1. Reason for Policy

Introduction

Scottish Water's responsibility to protect the privacy of our people and customers and safeguard the valuable data and information entrusted to us, is a vital part of our vision to be Trusted to Serve Scotland.

Understanding this responsibility and adopting the correct behaviours and procedures helps ensure that we process Personal Data, as defined by the relevant Data Protection Legislation, lawfully, transparently and securely, with the necessary controls in place. The highest standards of Data Protection are at the heart of how we do business to ensure we protect our reputation and fulfil our obligations to protect the rights and interests of our people and customers when processing Personal Data.

This policy promotes good practice and observance of Data Protection Legislation by everyone who works for or on behalf of Scottish Water, setting out the responsibilities of Scottish Water and its people to ensure compliance with the relevant UK and EU Data Protection Legislation.

Commitment

Scottish Water will:

- Implement appropriate controls to ensure that its Processing of Personal Data is compliant with this policy and be able to demonstrate this.
- Publish its corporate Privacy Notices on the Scottish Water Website and Intranet to ensure transparency regarding the types of Private and Personal Data we hold and the purposes for which we hold it.
- Require all third parties, where appropriate, with whom it shares data to abide by this policy and maintain the appropriate levels of security, privacy, control and protection of all shared data assets.
- Communicate any updates and changes to this policy and its privacy practices to customers, employees and associated third parties in a timely manner.

2. Scope

This policy applies to:

- All Private and Personal Data , which requires enhanced levels of control as identified by its security classification, that is collected, created, used, stored, transferred, archived or destroyed.
- All structured and unstructured Private and Personal Data that is processed by Scottish Water irrespective of whether it is held in digital systems and databases or in physical paper based storage, unstructured documents such as images, reports and spreadsheets, in e-mails or resides on digital media or devices and including verbal discussion.
- All Scottish Water employees and contingent workers (e.g. contractors, secondees, consultants, partners, service providers, vendors, related third parties) who, with appropriate authorisation, are provided with access to the Scottish Water digital technology, data assets and communications facilities they need to complete their job.
- Any third parties, where appropriate, with whom Scottish Water shares data for statutory, regulatory or other business purposes, subject to contractual agreement on how we protect shared data.

3. DEFINITIONS

Automated Processing

Any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent

Agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller

The person or organisation that (either alone or jointly or in common with other persons or organisations) determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the Data Protection Legislation.

Data Privacy Impact Assessment (DPIA)

Tools and assessments used to identify and reduce risks of a data processing activity.

Data Processor

This refers to any person (other than an employee of the Data Controller), public authority, agency or other organisation which Processes Personal Data on behalf of the Data Controller.

Data Subject

A living, identified or identifiable individual who is the subject of Personal Data held by Scottish Water.

Disclosure

Meaning transmission, dissemination or otherwise making data available by any means including:

- Verbally by discussion (e.g. talking about customers)
- Verbally by telephone (e.g. providing customer information over the phone)
- Physically - informally (e.g. displaying a post-it containing customer information)
- Physically (e.g. leaving a letter containing customer information unattended on a desk)
- Electronically (e.g. by email, file transfer, blog, social media).

Data Protection Legislation

The General Data Protection Regulation 2016 and the Data Protection Bill 2017 (collectively, GDPR) replaces the EU Data Protection Directive of 1995 and supersedes the Data Protection Act 1998.

Information Commissioner's Office (ICO)

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Personal Data

Any information relating to an identifiable person.

All Personal Data must be marked with the security descriptor of ***PERSONAL***, e.g. *SW Private – PERSONAL*.

Personal Data Breach

Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organizational safeguards that Scottish Water or our third party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notices

Separate notices setting out information that may be provided to Data Subjects when Scottish Water collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Private Data

Any data of a strategic, or operational or other nature of very high sensitivity where unauthorised Disclosure may have significant legal, regulatory, commercial, reputational or security repercussions.

All Private Data must be marked with the security classification of ***SW Private***.

Processing or Process

Any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised

Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the individual, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Category Data

Data revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

All Special Category Data must be marked with the security classification of ***SW Private – PERSONAL***.

4. POLICY DETAILS

How we protect Private and Personal Data

Scottish Water uses Personal Data to initiate, provide and maintain services. We may share, disclose, and transfer Personal Data with third parties only in order to initiate, provide, and maintain services, features and support.

Some Personal Data is considered to be of a Special Category. Such data is more personally sensitive and requires additional protection where it relates to race or ethnic origin, political opinions, religion or beliefs, trade-union membership, genetic data, health or sex life, criminal convictions or related security measures.

Scottish Water will Process all Personal Data in accordance with the following data protection principles as set out in Data Protection Legislation.

Personal Data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected only for specified, explicit and legitimate purposes
- Adequate, relevant and limited to the minimum necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security
- Not transferred to another country outside the EU without appropriate safeguards being in place
- Made available to Data Subjects who can exercise certain rights in relation to their Personal Data

The lawful reasons for much of Scottish Water's Personal Data Processing are due to our obligations to fulfil services or provide for a contract for our customers or employees, or the need to comply with a statutory or legislative requirement. Processing in these circumstances does not rely on Data Subjects' Consent. When Consent from the Data Subject is the lawful basis for Processing, Scottish Water will be explicit to the Data Subject that they can choose whether or not to give consent to Processing of their Personal Data.

Scottish Water will apply a security classification of ***SW Private*** to all Private Data and have appropriate controls to prevent unauthorised Disclosure. Personal Data will have a security descriptor of ***PERSONAL*** added, and may have additional security controls applied. For more information, see the *SW Information Asset Classification Standard*.

The appropriate privacy, protection and verification of use throughout the data lifecycle from collection, usage, storage, transfer, archive and destruction is critical to Scottish Water. In order to operate our business to the highest possible standard, Scottish Water will implement this policy to manage our customer, people, asset, financial, reporting, measurement and analytical data in accordance with our statutory and regulatory obligations.

In order to protect Private and Personal Data against unauthorised Disclosure, Scottish Water will:

- Ensure all Private and Personal Data is properly classified and labelled.
- Provide our staff with the appropriate level of access, awareness and training.
- Fulfil our obligations with regard to putting in place measures to protect Private and Personal Data, documenting these measures and verifying that these measures are effective.
- Abide by its obligations to maintain the privacy of all Personal Data held about customers, employees, non-employees, suppliers, partners and other third parties.
- Ensure the appropriate level of access control is applied for each Scottish Water person with authorised access permissions.

Scottish Water's Responsibility

Scottish Water is both a Data Controller and a Data Processor under Data Protection Legislation and all Scottish Water staff must ensure that they are aware of their responsibilities regarding data protection.

Although Scottish Water has a general responsibility for data protection under Data Protection Legislation, all Scottish Water leaders are responsible for the Personal Data they collect concerning Scottish Water employees and how it is used. Further, all individuals are responsible for ensuring that any Personal Data about themselves that they supply to Scottish Water is accurate and kept up to date.

If any member of Scottish Water staff identifies that they are, or are likely to be, engaged in collecting, handling or processing Private or Personal Data that is not currently security categorised, they must inform their line manager to ensure that Scottish Water is able to assist in safeguarding compliance.

Data Subjects' Rights and Requests

Scottish Water will respect the rights of Data Subjects with regard to any Personal Data that is held about them and how that data is Processed.

Data Subjects' rights include the right to:

- Receive certain information about Scottish Water Processing activities
- Request access to their Personal Data that we hold
- Prevent our use of their Personal Data for direct marketing purposes
- Ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed
- Ask us to rectify inaccurate Personal Data or to complete incomplete Personal Data
- Where Consent is the lawful reason for Processing, the right to withdraw Consent to Processing at any time
- Restrict Processing in specific circumstances
- Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest
- Request a copy of an agreement under which Personal Data is transferred outside of the EU
- Object to decisions based solely on Automated Processing, including profiling
- Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else
- Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms
- Make a complaint to the supervisory authority and
- Receive or ask for, in limited circumstances, their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

Scottish Water staff will verify the identity of any individual requesting Personal Data under any of the rights listed above and will not allow third parties to persuade them to disclose Personal Data without proper authorisation.

Scottish Water staff will immediately forward any Data Subject access request received to the Corporate Data and Compliance Team and comply with Scottish Water's Data Subject response process.

Consent

Scottish Water will ensure that Data Subjects are clear when they can choose to give or withhold their agreement to their Personal Data being collected and used in the manner and for the purposes presented to them. Most Personal Data Processing done by Scottish Water, for example, where we require Personal Data to provide a service or comply with a contract, will not rely on Data Subject Consent.

Where Consent is an option and is granted, Scottish Water will ensure that this is a freely given, specific, informed and unambiguous indication of that individual's wishes. Any Consent sought will be presented as separate from other terms and conditions and will not be a precondition of signing up to a service.

Where seeking Consent to collect and Process sensitive Personal Data, this must be explicit. It must be very clear and specific as to what type of data is to be collected or Processed, the purposes of the Processing and any special aspects that may affect the individual, such as any disclosures that may be made.

Consent must not be inferred; the Data Subject must indicate their consent for their Personal Data to be Processed by a clear, affirmative action and where Consent has been given, Data Subjects also have the right to withdraw Consent at any time.

Privacy Notices

Scottish Water is committed to transparency and providing accessible information to individuals about how we will Process their Personal Data. The most common way to provide this information is in a Privacy Notice. Therefore, prior to the collection and Processing of Personal Data, Data Subjects will be informed of the following via a Privacy Notice, published on the Scottish Water website and intranet:

- Who we are and how to contact us about any Personal Data we hold about you
- Why we collect and use your Personal Data
- How long we will keep your Personal Data
- How and when (if at all) Personal Data will be shared with third parties

On the Scottish Water website and intranet we also publish information about what your rights are in regard to the Personal Data we hold, including:

- Your right to access your Personal Data
- Your right to withdraw consent to collection and Processing where consent is the lawful reason for processing
- Your right to rectify any Personal Data erased
- Your right to restrict Processing, and
- Your right to lodge a complaint.

We will also inform you:

- If any Personal Data is to be transferred outside of the EU and how this affects you
- Of any Automated Processing, such as profiling, that will be performed on the Personal Data we Process about you
- If the Personal Data must be supplied to fulfil or enter into a contract with us
- If there are any possible consequences of failing to provide Personal Data, and
- Of any other information that would make the processing of your Personal Data clear, understandable and fair.

Reporting a Personal Data Breach

Scottish Water has a robust data security alert process to deal with any suspected Personal Data Breach and will notify Data Subjects and/or the Information Commission Office (ICO) where we are legally required to do so. Scottish Water will notify the ICO of any serious breach within 72 hours as stipulated by Data Protection Legislation. Data Subjects, where identified, will be notified without delay.

All employees and relevant third parties are fully aware of their obligations to report any leak or potential leak of Personal Data.

To mitigate the risk of data loss, all Scottish Water mobile IT equipment is fitted with contemporary cyber encryption and/or password controls.

5. Accountability and Governance

In order to minimise the risk of data security breaches and uphold the protection of Private and Personal Data, Scottish Water have implemented a comprehensive set of governance measures and good practice tools.

Scottish Water will:

- Maintain data inventories to ensure the on-going corporate assessment of all Personal Data Processed and/or held
- Ensure consistent corporate assurance and education
- Undertake, assure and approve Data Privacy Impact Assessments
- Protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

For more information see Annex A: *Personal Data Inventories*, Annex B: *Corporate Assurance and Education* and Annex C: *Private Data Handling.*

Scottish Water business functions will be accountable for demonstrating that the Processing of Private and Personal Data is compliant with this policy and for developing and delivering appropriate functional level training for their people over and above the corporate training and education provided.

All Scottish Water employees, contractors, consultants, partners and contingent workers must ensure that they understand and fulfil their personal responsibility in the protection of any Private and Personal Data processed in performance of their duties as set out in this policy and in accordance with the processes implemented in their business function. All Scottish Water employees and contingent workers have a responsibility to participate in essential corporate awareness and other training in this area.

Scottish Water's Data Protection Officer will approve all Data Privacy Impact Assessments.

Scottish Water's Business Information Group will provide collective senior leadership, direction, implementation of strategy and approval of all data and information management related policy.

The Information and Data Approval Board will be accountable for the approval of Data Privacy Impact Assessments, assurance of privacy, protection and quality by design and review of data breach recommendations.

In summary, we will:

- Adopt processes and implement measures which demonstrate compliance with this policy, especially with regard to documentation, data security and data protection by design/default
- Verify the operational effectiveness of processes and measures to ensure compliance.

6. Roles and Responsibilities

Data Protection Officer

The Scottish Water Data Protection Officer (DPO) is a member of the Scottish Water Executive Leadership Team and is accountable to the Scottish Water Board of Directors for the management of Personal Data within Scottish Water and for ensuring compliance with both Data Protection Legislation and good practice in the management of data.

The DPO, who the Board considers to be suitably qualified and experienced, has been appointed to take responsibility for Scottish Water's compliance with this policy on a day to day basis and in particular, has direct responsibility for ensuring that Scottish Water complies with Data Protection Legislation.

The DPO is responsible for ensuring maintenance of the annual registration of Scottish Water in the public register of Data Controllers; for reviewing details of such notification in light of any changes to Scottish Water data processing activities and for any additional requirements identified by means of a Data Protection Impact Assessment.

The DPO will ensure that all individuals receive annual mandatory training and general awareness of their responsibilities in regard to Data Protection Legislation.

The DPO will be supported in these tasks by the Scottish Water Corporate Data and Compliance Team.

- DPO Contact details are: Data Protection Officer, Scottish Water, Castle House, Carnegie Campus, Dunfermline, KY11 8GG or email DPO@scottishwater.co.uk

Corporate Data and Compliance Team

Scottish Water's Corporate Data and Compliance Team will support the DPO and our wider business by:

- Informing and advising Scottish Water on its data and information management obligations
- Monitoring policy compliance and initiating data and information management improvements
- Embedding Scottish Water's data and information management policies, standards, processes
- Developing and launching training, communications and engagement campaigns for our people
- Undertaking and responding to data and information management related audits
- Ensuring adequate data and information privacy, protection and quality by design
- Managing processes related to Data Subject requests and supporting data collection to fulfil freedom of information requests
- Ensuring that Scottish Water holds appropriate documentation on the Private and Personal Data that it processes.

7. VIOLATIONS

Failure to comply with this policy may result in Scottish Water failing to meet its statutory obligations; suffering from commercial or reputational damage, loss of customer trust and significant fines being imposed by the ICO.

Failure to comply with this policy may result in disciplinary action being taken against the individuals involved, which could include the withdrawal of permission to use Scottish Water digital technology and communications facilities, and in serious cases, dismissal. In the case of contractors, consultants and contingent workers, Scottish Water may terminate their contract.

ANNEX A. PERSONAL DATA INVENTORIES

These data inventories will hold and evidence the following:

- The lawful reason for processing the data set
- The appropriate classification for the data set
- How we will ensure that data is accurate, and, where it is inaccurate, how it will be corrected
- Details of the data archive, retention and disposal processes
- Access controls
- Appropriate treatment of contracts with any third party who processes Personal Data on behalf of Scottish Water
- An appropriate level of anonymizing Personal Data held in non-production systems (e.g. test data)
- Identification of all data integrations, including utilisation within business reporting, measurement and analytics.

ANNEX B. ASSURANCE AND EDUCATION

Scottish Water will ensure consistent corporate assurance and education and evidence the following:

- Training, communication and engagement campaigns involving our people
- An appropriate level of governance and change control to ensure
    - maintenance of the data inventories
    - the undertaking and review of Data Privacy Impact Assessments
    - appropriate corporate Scottish Water approval of change
- An adequate level of support for our business areas and people to ensure compliance with our policies and processes
- An appropriate level of protection for any Private and Personal Data processed by others on our behalf or transferred outside the EU
- Assurance and approval of Data Privacy Impact Assessments related to all process, system and data change.

ANNEX C. PRIVATE DATA HANDLING

The following requirements pertain to the collection, use, storage, transfer and destruction of all Private Data:

- Limit Collection and Storage

  The collection and storage of Private Data must be limited to that which is relevant and necessary to support the operational outcomes or our business. Where data exists in systems or business processes where it is not required, it should be eliminated.

- Access Control

  The ability to collect, store, use, transfer, and destroy Private Data must be strictly limited to those individuals who require it to perform their job responsibilities i.e., on a "need to know" basis. This applies to both digital and physical data stores.

- Administrator Access

  Enhanced access to digital tools that store or use Private Data must be administered and controlled by approved access control procedures, including adequate commercial segregation controls.

- Audit Trail

  Systems storing Private Data must log any transaction that results in the creation, modification, or deletion of Private Data elements. These log files will be reviewed on a regular basis to identify any unauthorised or suspicious activity.

- Display Control

  Digital tools must only display the minimal amount of Private Data necessary for business purposes.

- In Transit

  All Private Data that is transmitted externally outside of Scottish Water's network must be protected by Scottish Water approved means.

- Third Party Access

  The transfer of Private Data to third parties must be limited to that which is necessary to support the business relationship with the third party. Scottish Water must establish security and privacy contractual requirements with all third parties that will be handling Scottish Water Private Data. Contractual requirements may include; the secure handling of data, security incident reporting, due diligence and the right to audit.

- At Rest

  All Private Data that is stored in a digital system or by physical storage must be protected by Scottish Water approved means. Physical measures include a locked cabinet, locked drawer, secure room or safe until they are destroyed.

- Retention and Disposal

  Private Data, if required for management approved business purposes, should be retained and then securely destroyed according to the SW Data Retention Policy.

- Archives

  Private Data archives where they be online, offline or hardcopy archives must be protected by approved means using methods similar to those used to protect production data such as encryption or access control.