|  |
| --- |
| information manAgement policy |
|  |
| **Governance Framework**  Version 5 |
|  |

May 2023

CONTENTS

Contents

[1. RECORDS MANAGEMENT POLICY 4](#_Toc126763115)

[1.1. INTRODUCTION TO RECORDS MANAGEMENT 4](#_Toc126763116)

[1.2. MEANING OF RECORD 5](#_Toc126763117)

[1.3. THE PRINCIPLES OF THE RECORDS MANAGEMENT POLICY 5](#_Toc126763118)

[1.3.1. Roles and Responsibilities 5](#_Toc126763119)

[1.3.2. Office wide management and destruction of information 6](#_Toc126763120)

[1.4. MANAGEMENT OF ELECTRONIC RECORDS 7](#_Toc126763121)

[1.4.1. Electronic records 7](#_Toc126763122)

[1.4.2. Accessibility and storage of electronic records 7](#_Toc126763123)

[1.5. TRAINING AND AWARENESS 9](#_Toc126763124)

[2. DATA PROTECTION 10](#_Toc126763125)

[2.1. INTRODUCTION TO DATA PROTECTION 10](#_Toc126763126)

[2.1.1. The Data Protection Principles 10](#_Toc126763127)

[2.2. PERSONAL DATA PROCESSING 10](#_Toc126763128)

[2.3. HANDLING PERSONAL DATA 11](#_Toc126763129)

[2.4. DOCUMENTATION AND RECORDS 12](#_Toc126763130)

[2.5. ENFORCEMENT BY THE INFORMATION COMMISSIONER 12](#_Toc126763131)

[2.6. COMPLIANCE AND REVIEW 13](#_Toc126763132)

[2.7. CHANGES TO PERSONAL DETAILS 13](#_Toc126763133)

[3. BREACH REPORTING 14](#_Toc126763134)

[3.1. REPORTABLE BREACHES 14](#_Toc126763135)

[3.2. ROLE OF DATA PROCESSORS 14](#_Toc126763136)

[3.3. REPORTING A BREACH 14](#_Toc126763137)

[3.4. INFORMING INDIVIDUALS 15](#_Toc126763138)

[3.5. OTHER REQUIREMENTS 15](#_Toc126763139)

[4. ACCESS TO INFORMATION 17](#_Toc126763140)

[4.1. INTRODUCTION TO ACCESSING INFORMATION 17](#_Toc126763141)

[4.2. UK GDPR AND DATA PROTECTION ACT 2018 17](#_Toc126763142)

[4.2.1. How to recognise a subject access request 17](#_Toc126763143)

[4.2.2. How to find information 19](#_Toc126763144)

[4.2.3. Information to be provided in response to a request 20](#_Toc126763145)

[4.3. FREEDOM OF INFORMATION (SCOTLAND) ACT 2002 20](#_Toc126763146)

[4.4. ENVIRONMENTAL INFORMATION (SCOTLAND) REGULATIONS 2004 21](#_Toc126763147)

[4.4.1. OUR fOISA and eisr principles 21](#_Toc126763148)

[4.4.2. Our disclosure log 21](#_Toc126763149)

[4.4.3. ROLES AND Responsibilities 22](#_Toc126763150)

[5. RECORDS RETENTION 23](#_Toc126763151)

[5.1. CREATING AND DISCLOSING INFORMATION 24](#_Toc126763152)

[5.2. RETENTION OF RECORDS 24](#_Toc126763153)

[5.3. STORAGE OF RECORDS 25](#_Toc126763154)

[5.4. RETRIEVING RECORDS 26](#_Toc126763155)

[5.5. DESTROYING RECORDS 27](#_Toc126763156)

[5.6. MONITORING AND REVIEW 28](#_Toc126763157)

[6. RECORDS MANAGEMENT DEFINITIONS 29](#_Toc126763158)

[APPENDIX 1: RECORD TYPES AND RETENTION PERIODS 30](#_Toc126763159)

# RECORDS MANAGEMENT POLICY

## INTRODUCTION TO RECORDS MANAGEMENT

Information and records management is necessary to support our employees in understanding best practice and legal requirements aligned to the creation, processing, storage and disposal of our records. This policy is available to help employees understand their responsibilities. By following this policy and any supporting guidance, employees will be able to effectively manage the records they are responsible for.

As a public authority, we are covered by Section 61 of the Freedom of Information (Scotland) Act 2002. This requires Scottish Ministers to issue a code of practice setting out their expectations in relation to keeping, managing, and destroying records. Ministers must have regard to the public interest in allowing public access to information that Scottish public authorities hold.

The Scottish Government’s code of practice for public bodies in Scotland forms the basis of our policies and processes surrounding the way we manage our records.

We are also subject to the Public Records (Scotland) Act 2011. The Act requires specific public bodies to set out proper arrangements for managing their records. WICS has a records management plan which we submitted to the Keeper of the National Records of Scotland in 2016. The plan was agreed on an ‘improvement basis’. This means that we had identified gaps in our compliance, but the Keeper could see we had evidenced commitments to closing those gaps in due course.

We recognise that managing our knowledge, information and records efficiently will:

* support our work
* facilitate good governance arrangements
* help us manage risk, and
* help us to comply with our legal obligations.

Records are vital to our past, present, and future work. They show the decisions we have made, and the steps taken towards those decisions. They must therefore be managed systematically from creation to disposal. Records also help us maintain professional standards and use best practice.

The main aim of this policy is to set out practices that should be followed in relation to the creation, retention, management and final disposition of all records.

## MEANING OF RECORD

Records can be held in a variety of ways and on different media, electronic and manual. Within this policy, reference to a "record" means information stored on any media. It is crucial to remember that records are not confined to hard copy papers and will include anything on which information is recorded in a tangible form, or which may be made tangible by using equipment. The definition therefore encompasses hard copy papers, emails, electronic files, photographs, hand-written notes, tape recordings/transcripts, films, and computer databases containing information that can be retrieved in readable form.

## THE PRINCIPLES OF THE RECORDS MANAGEMENT POLICY

### Roles and Responsibilities

Records management is the responsibility of all of us at WICS. This means we all need to think about the information we collect, create, store, share, and disposes of.

Senior Management Responsibility

Overall responsibility for the enforcement of this records management policy lies with the Director of Corporate and International Affairs, Donna Very.

Records Manager Responsibility

Supporting the senior manager and leading on operational activity is the Information Manager. The Information Manager is further supported by the data protection officer (DPO) and information asset owners (IAO).

Data protection officer (DPO)

The data protection officer is responsible for educating everyone about data compliance and helps to ensure appropriate training is sought and rolled out.

Information asset owner (IAO)

The information asset owner is the individual responsible for the running of each function within WICS. Their role is to understand what information is held within that area of business, and how it is managed.

Together, we should all make sure that records are:

Authentic

Records must be reliable. It must be possible to prove that records are what they purport to be and that the individual who created them is known. With electronic records, changes and additions must be identifiable through audit trails.

Accurate

Records must accurately reflect the transactions and other business activities they describe.

Accessible and usable

Records should be readily available when needed. It should be possible for people who have appropriate authority to use and rely on records for as long as they are required.

Complete

The content, context and structure of records must be sufficient such that it is possible to reconstruct the activities and transactions they describe. It must be possible to identify any alterations made to records post creation, together with the identity of the member(s) of staff who made the alterations.

Comprehensive

Records must be capable of being easily understood and should provide clear information about the relevant business activity.

Compliant

Records must comply with any record keeping requirements resulting from legislation, audit rules, professional standards, and other relevant regulations.

Effective

Records must be maintained for specific purposes and the information contained in them must meet those purposes.

Secure

Records must be securely maintained using appropriate physical and technical measures to prevent unauthorised access, alteration, damage, or destruction. They must be stored in a secure environment, the degree of security reflecting the sensitivity and importance of the contents. Where records are migrated across changes in technology, the evidence preserved must remain authentic and accurate.

### Office wide management and destruction of information

Our records naturally fall within the key business functions which are headed up by our IAOs. All records, regardless of their age, must be maintained in such a way that they are easy to find and to retrieve. This will be achieved by all employees ensuring that they are familiar with our SharePoint document repository.

Appendix 1 of this policy sets out applicable retention periods for our records.

When dealing with records, we must be mindful of our duties under other related legislation, for example:

* the UK General Data Protection Regulation (UK GDPR)
* Data Protection Act 2018 (DPA)
* Freedom of Information (Scotland) Act 2002 (FOISA), and
* Environmental Information (Scotland) Regulations 2004 (EISRs).

Under the UK GDPR and the DPA, a Scottish public authority that processes personal data is deemed to be a data controller. The data controller remains responsible for personal data contained in a record until its destruction.

Before a record is destroyed, we must establish whether the record is subject to a request for information under the FOISA, or under the EISRs. In such instances, it is an offence to destroy a record that is known to be the subject of a request. Destruction must be delayed until disclosure has taken place. Alternatively, if we have decided not to disclose the information, destruction must be delayed until the review and appeal provisions have been exhausted. The only exception to this is if the circumstances are such that it is not reasonably practicable to stop the destruction from taking place.

## MANAGEMENT OF ELECTRONIC RECORDS

### Electronic records

The main issues when managing electronic records are the same as those when managing any record. This includes creating authentic records, tracking records and having appropriate arrangements in place for disposing of records.

Most of WICS records are held electronically. Take care to ensure the authenticity of electronic records, which can easily be manipulated. This is relevant in relation to our responsibilities under the FOISA which states that there should be no question as to the authenticity of any information we release. Furthermore, the authenticity of an electronic record will be a key factor in determining whether the record is admissible in a court of law. Therefore, WICS must have in place appropriate procedures which ensure the authenticity of electronic records.

### Accessibility and storage of electronic records

It is reasonable to expect that people across and between teams will need to access a record. We have appropriate controls in place to ensure financial records, or those of a sensitive nature, are restricted.

Electronic records should be saved in the appropriate place. Duplication of records should be avoided. Records should be saved on our Microsoft Office 365 cloud portal, which consists of SharePoint sites. You may also save records within Office 365 individual user OneDrive’s. You should only save records on your desktop or laptop computer temporarily. Anything stored locally should be deleted as soon as possible or moved to our Office 365 portal.

Calendars

Calendar entries are a form of record and so are subject to FOISA requests. It is possible to make personal entries, but these should be stored as a private entry to indicate that it is of a personal nature. Like all other records, calendar records have a lifecycle, and will be deleted automatically after a period of no more than 6 months following the event.

Teams

Teams chat messages and posts are a form of record and are also subject to FOISA requests. Teams chat messages and posts have a lifecycle like all other records and will be automatically deleted after a period of no more than 30 days.

Emails

Emails are too a form of record subject to FOISA requests and should therefore be considered in the same way as any other record. All emails will be automatically deleted from an individual’s inbox after 6 months. Any email that individuals wish to retain for more than 6 months should be moved to an Outlook folder tagged with a 6-year retention label. In this circumstance, Outlook will retain the email for 6 years from the date sent, or date of receipt. You should review your emails on a regular basis, deleting anything you no longer need.

SMS text messaging and social media

Consideration should be given to records that are created using SMS text messaging and social media (such as Twitter and LinkedIn). These records are subject to the same regulations as other formats of records and should be captured, retained, and managed appropriately. You should apply the same 30-day retention policy to text messaging and other social media communications.

Backups

Microsoft Office 365 employs multiple layers of redundancy and backups of information at the datacentre level. This means that in a rare event where data is lost or corrupted on Microsoft servers, it can be restored. This includes all mailboxes, contacts, etc.

## TRAINING AND AWARENESS

It’s important that everyone understands their responsibilities, as set out in this policy. We provide regular training to ensure all staff understand their obligations regarding records management, data protection, data security and freedom of information.

# DATA PROTECTION

## INTRODUCTION TO DATA PROTECTION

We recognise the importance of making sure that personal data is handled in accordance with the requirements set out in the DPA and the UK GDPR.

If an employee does not safeguard personal data properly this might result in disciplinary action being taken against them.

Data Protection Legislation (DPL) regulates the collection, storage, processing, use (including disclosure) and destruction of information relating to an identified or identifiable living individual. This information is known as personal data, and the individual is known as the data subject.

### The Data Protection Principles

The DPL contains rules that you will need to follow when processing personal data. These rules as known as the data principles. They state that personal data must:

* Be processed fairly, lawfully and in a transparent manner. This means that it must be made clear to data subjects that personal data about them is being processed and the purposes for it. We provide data subjects with transparency statements for this purpose.
* Be obtained only for specific, explicit and legitimate purposes and should not be processed in any manner incompatible with those purposes. This means that personal data collected for one purpose cannot be used for a different, unrelated purpose.
* Be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.
* Be accurate and where necessary, kept up to date.
* Not be kept in a form that makes it possible to identify data subjects for longer than is necessary for the purposes for which the data is processed.
* Kept secure by means of appropriate technical and organisational safeguards.

## PERSONAL DATA PROCESSING

Before we process any personal data for the first time, we must review the purposes of the processing activity and select the most appropriate lawful basis under the DPL. We document information about the purposes, lawful basis and special conditions (if applicable) of the processing, within our transparency statements which are available on PeopleHR.

We use employees’ personal data to carry out our role as employer, for example to enable us to meet our responsibilities under the employment contract and pay your salary. Full details can be found in our employee transparency statement, which is available on PeopleHR.

Under the DPL, processing certain information, known as Special Category Data, is subject to special restrictions. Processing Special Category Personal Data is prohibited unless an exception applies under the DPL. If you have any questions about whether information held constitutes Special Category Data and whether there are any exceptions under the DPL, please speak to the Data Protection Officer (DPO).

## HANDLING PERSONAL DATA

By managing data appropriately and using the right controls, we will:

* fully observe the conditions regarding the fair collection and use of personal data
* meet our legal obligations to specify the purpose(s) for which personal data is used
* collect and process appropriate personal data and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
* ensure the quality of personal data used
* take appropriate technical and organisational security measures to safeguard personal data
* ensure that personal data is not transferred outside the UK without suitable safeguards; and
* ensure that the rights of people whose data we hold are respected and that they can fully exercise their rights under the DPL and against WICS.

We will also ensure that:

* someone is appointed to the role of DPO
* everyone managing and handling personal data understands their responsibilities for following good data protection practice and complying with the DPL
* everyone managing and handling personal data is appropriately trained to do so
* queries and complaints about handling personal data are promptly and courteously dealt with; and
* data processing by third parties on our behalf is carried out under a written agreement.

In accordance with our IT Security Policy, we will take steps to ensure that personal data is always kept secure against unauthorised or unlawful loss or disclosure.

All contractors, consultants, partners, other associates or agents who process personal data on our behalf as processors must enter into a contract that provides (as a minimum) that they:

* only act on our written instructions (unless required by law to act without)
* ensure people who process personal data on our behalf are subject to a duty of confidence
* only engage a sub-contractor to process personal data on our behalf with our prior consent and a written contract
* assist us in responding to requests from data subjects seeking to exercise their rights under the DPL
* assist us in meeting our obligations under the DPL in relation to security of processing, the notification of personal data breaches and data protection impact assessments where applicable
* delete or return all personal data to us as requested at the end of the contract
* allow data protection audits and inspections by us of personal data held on our behalf (if requested) to ensure that both parties are meeting their requirements under the DPL and to tell WICS immediately if asked to do something that infringes the DPL; and
* indemnify us against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

## DOCUMENTATION AND RECORDS

We maintain a business classification scheme and retention schedule which is a register of the records WICS processes. It outlines the type of data held, its classification and which IAO is responsible for it. It also includes other details, for example whether the record is personal, shared, or vital to the functioning of WICS. We also record retention periods here.

We have a suite of transparency statements which we issue to ensure that data subjects understand how we collect, use, store, share and delete their personal data.

We take appropriate measures to provide any information we share in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Our transparency statements are available on the corporate website and on the Scotland on Tap website.

## ENFORCEMENT BY THE INFORMATION COMMISSIONER

The Information Commissioner has certain enforcement powers and may serve enforcement notices on an organisation where it considers that the Data Protection Principles have been breached. There are potential financial penalties and compensation payments due following failure to comply with the DPL. In the unlikely event that you receive an enforcement notice or any other correspondence from the ICO, please refer this immediately to our DPO.

## COMPLIANCE AND REVIEW

This policy is extremely important. Any breach of the policy, or of the Data Protection Principles, will be dealt with under our disciplinary procedures, which can be found in our Employee Handbook. In certain circumstances, a breach of this policy, or of the Data Protection Principles, may be considered gross misconduct and may result in immediate termination of employment or engagement without notice or payment in lieu of notice.

We review this policy and associated procedures on a regular basis to ensure they meet all legislative and regulatory requirements and best practice guidance. In addition, an annual data protection audit is carried out to ensure ongoing compliance with the provisions of the DPL.

## CHANGES TO PERSONAL DETAILS

It is in your own interest to keep your personal details up to date. Any changes should be processed through PeopleHR immediately. Contact your line manager if you need any help with this. Fraudulent claims relating to personal details may result in disciplinary action and may lead to dismissal.

# BREACH REPORTING

## REPORTABLE BREACHES

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people’s rights and freedoms. If it is likely there will be such a risk, then we must notify the ICO. If it is unlikely there is no requirement to report the breach to the ICO.

In assessing risk to people's rights and freedoms, it is important to focus on the potential negative consequences for individuals. A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. We will assess this case by case, looking at all relevant factors.

If you become aware of a breach, you should immediately notify the Records Manager who will work with the DPO and take steps to contain it. The DPO will assess the potential adverse consequences for individuals.

## ROLE OF DATA PROCESSORS

If we use a data processor, and the processor suffers a personal data breach, under Article 33(2) of the UK GDPR the processor must tell us without undue delay as soon as it becomes aware of the breach.

Where we engage a data processor, the requirements on breach reporting will be detailed in the contract between us and the processor, as required under Article 28 of the UK GDPR.

## REPORTING A BREACH

We are under an obligation to report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If we take longer than this, we must provide reasons for the delay to the ICO.

When reporting a breach, the UK GDPR says controllers must provide:

* a description of the nature of the personal data breach
* the name and contact details of the DPO
* a description of the likely consequences of the breach; and
* a description of the measures taken, or proposed to be taken, to deal with the breach.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So, Article 33(4) of the UK GDPR allows controllers to provide the required information in phases, if this is done without undue further delay.

The ICO expects controllers to prioritise the investigation, provide adequate resources, and expedite the investigation urgently.

The ICO can be notified of a breach via their website or breach reporting helpline.

## INFORMING INDIVIDUALS

If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR says controllers must inform those concerned directly and without undue delay.

A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. Again, we will assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a personal data breach, such as financial loss and identity theft.

If we decide not to notify individuals, we must still notify the ICO unless we can demonstrate that the breach is unlikely to result in a risk to rights and freedoms of individuals. The ICO has the power to compel controllers to inform affected individuals if it considers that there is a high risk. In any event, we will document our decision-making process.

When informing individuals of a breach, we must describe, in clear and plain language, the nature of the personal data breach and, at least:

* the name and contact details of our DPO
* a description of the likely consequences of the personal data breach; and
* a description of the measures taken, or proposed to be taken, to deal with the breach including information about the measures taken to mitigate any possible adverse effects.

## OTHER REQUIREMENTS

Our Records Manager and DPO will ensure that all personal data breaches are recorded, regardless of whether they need to be reported to the ICO or affected individuals.

Article 33(5) of the GDPR requires us to document the facts relating to the breach, its effects and the remedial action taken. This is part of our overall obligation to comply with the UK GDPR’s accountability requirements. It allows the ICO to verify our compliance with its notification duties under the UK GDPR.

As with any security incident, we will investigate whether the breach was a result of human error or a systemic issue. We will also investigate how to prevent a recurrence – whether this is through better processes, further training, or other corrective steps.

Failing to notify a personal data breach when required to do so may result in a significant fine up to £8,700,000.

# ACCESS TO INFORMATION

## INTRODUCTION TO ACCESSING INFORMATION

We are committed to acting in an open and accountable way and to ensuring that we comply with our statutory obligations to make information available to individuals and the public at large.

This policy sets out our responsibilities in respect of providing access to personal data, environmental information and any other information requested via the Freedom of Information Act.

## UK GDPR AND DATA PROTECTION ACT 2018

Under the UK GDPR, data subjects have a general right to find out whether we hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request. The purpose of the right is to enable the individual to be aware of, and to verify, the lawfulness of the processing of personal data that we are undertaking.

Failure to comply with a subject access request would result in the individual being informed of the reasons why their request was refused, and their right to make a complain to the ICO.

Once a data subject access request is received, we must provide the information requested without delay and at the latest within one month of receiving the request. If a data subject access request is complex or the data subject has made numerous requests, we:

* **may extend the period of compliance by a further two months; and**
* **must tell the individual about the extension within one month of receiving the request and explain why the extension is necessary.**

### How to recognise a subject access request

A data subject access request may be made by an individual or by someone acting with the authority of an individual, for example, a parent making a request in relation to information relating to their child. The request may be:

* **to confirm whether we process personal data about him or her and, if so**
* **to ask for access to that personal data; and**
* **to request other supplementary information regarding such processing.**

Data subjects have the following rights in relation to their personal data:

* to be told about how, why and on what basis personal data is processed (as contained within our transparency statements)
* to access their personal data
* to have personal data corrected if it is inaccurate or incomplete – the DPL states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact
* to have personal data erased – this right only applies if:
* the personal data is no longer necessary for the purpose for which we originally collected or processed it
* we are relying on consent as our lawful basis for holding the personal data and the individual withdraws their consent
* we are relying on legitimate interests as our lawful basis, the individual objects to the processing of their personal data, and there is no overriding legitimate interest to continue this processing
* we are processing the personal data for direct marketing purposes and the individual objects to that processing
* we have processed the personal data unlawfully; or
* we must delete the personal data to comply with a legal obligation.
* to restrict the processing of personal data – this right only applies where:
* the accuracy of the personal data is contested, and we are verifying the accuracy of that data
* the processing of the personal data is unlawful (but the individual does not want the personal data to be erased)
* we no longer need the personal data, but the individual requires the data to establish, exercise or defend a legal claim; or
* the individual has objected to our processing their personal data and we are considering the objection
* to object to the processing of personal data where we carry out the processing for a task carried out in the public interest; to exercise official authority vested in us; or in pursuit of our or a third party's legitimate interest. The right to object is an absolute right in respect of personal data being processed for direct marketing purposes
* to obtain personal data provided to us by the individual for that individual's own reuse, where we process such personal data to perform a contract with that individual or where the individual has given consent and where the processing we do is undertaken by automated means; and
* to object to decisions being taken by automated means which produce legal effects concerning an individual or similarly significantly affect an individual.

Data subjects can seek to exercise the above rights against us in writing, by email or verbally. Such requests do not have to refer to the legislation, 'data protection' or 'personal data'. In fact, requests often cite the incorrect legislation (for example, they may refer to 'freedom of information' where they are seeking access to their own personal data). We must ensure that requests under the DPL are recognised so that we are compliant with the relevant statutory obligations.

If you receive a request relating to personal data, the request must be emailed immediately to our Information Manager and DPO via [DPO@wics.scot](mailto:DPO@wics.scot) so the request can be actioned within the time limit set down in the DPL. Where a data subject access request is received verbally, the employee taking the call must record the name and contact details of the individual and immediately email these details to [DPO@wics.scot](mailto:DPO@wics.scot). Our Information Manager, in conjunction with the DPO, is responsible for responding to all requests relating to personal data. You should not handle requests yourself unless advised to do so by the DPO.

If we fail to respond to a request from a data subject and are found to be guilty of an offence under the DPA, an investigation will be made as to the reasons for the failure to respond. Where appropriate, disciplinary action will be taken.

Any data subject can complain to us if they feel that we have:

* misused their personal data
* refused to allow access to data
* refused to amend alleged inaccuracies; or
* otherwise breached the DPL in relation to their personal data or data protection rights.

Data subjects may also raise complaints with the ICO.

### How to find information

The personal data we need to provide in response to a data subject access request may be in our electronic filing systems or on those of our processors or other third parties. For this reason, it is important to identify at the outset the type of information being asked for, so that the search can be focused.

Depending on the type of information being asked for, we may need to search all or some of the following:

* electronic systems, computers, backups
* manual filing systems, storage facility
* data systems held externally by our processors
* devices that employees use and others that fall within our IT Security Policy
* pensions data held by Falkirk Council Local Government Pension Scheme; and
* data held by any consultants engaged to provide assistance with performance management and/or disciplinary and grievance procedures.

Employees should search these systems using the individual's name or other personal identifier. Records must be kept of all the searches undertaken and the search results.

### Information to be provided in response to a request

Individuals are entitled to access the personal data we process about them and the following information:

* the purposes for which we process the personal data
* the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries (those countries outside the EU/EEA) or international organisations
* where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period
* the fact that the individual has the right:
* to request that we rectify, erase or restrict the processing of his/her personal data
* to object to its processing
* to lodge a complaint with the Information Commissioner's Office
* where the personal data has not been collected from the individual, any information available regarding the source of the personal data
* any automated decision we have taken about the individual, together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

The information referred to above should be provided:

* in a way that is concise, transparent, easy to understand and easy to access
* using clear and plain language, with any technical terms, abbreviations or codes explained
* in writing, if the data subject access request was made in writing; and
* in a commonly used electronic format, if the data subject access request was made electronically, unless otherwise requested by the individual.

## FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

FOISA provides individuals the right to ask for information that Scottish public authorities hold. Requests must be made in writing and the information will be provided within 20 working days, subject to exemptions.

We are fully committed to the aims of FOISA and related legislation and we make every effort to meet our obligations.

## ENVIRONMENTAL INFORMATION (SCOTLAND) REGULATIONS 2004

The Environmental Information (Scotland) Regulations 2004 ('EISR') provide individuals the right to request environmental information that Scottish public authorities hold. Requests must be made in writing and the information will be provided within 20 working days (which may be extended to 40 working days), subject to exceptions.

We are fully committed to the aims of EISR and related legislation and make every effort to meet our obligations.

### OUR fOISA and eisr principles

**At WICS, we:**

* **Support the legislations underpinning principles by encouraging open and transparent behaviour.**
* **Demonstrate commitment to FOISA and EISR by publishing as much information as possible on our website**
* **Support the effective application of FOISA and EISR, by creating and sharing information thoughtfully, deliberately, and purposefully.**

### Our disclosure log

Our Disclosure Log accompanies our Guide to Information and Publication Scheme, which we have a legal duty to maintain under FOISA.

As part of our commitment to be open and transparent, and in order to provide greater access to our information, we aim to publish all requests and responses. However, on some occasions this may not be possible. The FOI Officer will assess each request on a case by case basis to determine whether or not it should be published

All responses published on the Disclosure Log will be dealt with in accordance with the UK GDPR and the Data Protection Act 2018. For example, personal details, such as names and addresses (both postal and email), will be redacted to protect a requester’s privacy.

We aim to have an effective and coordinated approach to publishing information requests and responses on our Disclosure Log. We will always do so as soon as practically possible after the response has been sent to the requester.

Requests and response published on the Disclosure Log will be available forever as it is made public.

### ROLES AND Responsibilities

The roles and responsibilities of each category of employee is outlined below:

Freedom of Information Officer

* Develop, maintain, and monitor this policy, procedures and the Guide to information and publication scheme
* Consider what information we can proactively publish and include within our Guide to information and publication scheme
* Maintain the Disclosure Log, publishing requests as soon as practicably possible after the response has been sent
* Coordinate responses to requests for information in conjunction with Senior Management and Chief Executive
* Calculate any fees to be charged for FOISA requests, in line with our Freedom of Information Fees Scheme
* Provide advice and guidance on our policy and procedures
* Identify and communicate any FOI issues to Senior Management and Chief Executive
* Allocate the request for information to relevant member(s) of staff
* Ensure that requests for information are handled effectively by logging and co-ordinating requests
* Liaise with the DPO to prepare and finalise responses to requests for information

Senior Management

* Be aware of what FOISA and EISR means and the differences between the two
* Ensure all staff comply with the agreed policy and procedures for FOISA and EISR requests
* Provide assistance to and approval of any responses drafted by the FOI Officer

All staff

* Be aware of what FOISA and EISR means and the differences between the two
* Follow the policy and procedures for recognising and handling FOI requests, sending any request promptly to [FOI@wics.scot](mailto:FOI@wics.scot)
* Support the FOI Officer in dealing with all requests promptly, providing advice and assistance to requestors for information in line with best practice and guidance.

# RECORDS RETENTION

To comply with current statutory, legal and regulatory requirements, certain records have to be retained for a minimum period and, beyond that for no longer than is necessary for the purposes for which the record was created, or the organisation requires it. In many cases, it is an offence to destroy a record before a minimum time has elapsed.

This policy provides guidance on the minimum periods for which certain records should be retained, how they should be stored if they need to be retained for a period and how they should be destroyed.

In respect of maximum retention periods, the law is much less prescriptive. In most cases it is up to organisations to consider how much longer (than the statutory minimum period) their records ought to be maintained for their purposes.

In the context of freedom of information, data protection, litigation, or a regulatory investigation, the random destruction of or failure to retain records could give rise to an adverse inference. That risk may be managed if the retention and destruction of records has been carried out in accordance with an established policy based on sound commercial and legal reasoning and considerations. A structured approach is therefore essential.

The aims of this policy are to help us to:

* improve our information management practices
* comply with current statutory, legal and regulatory requirements on retention
* manage the risks associated with the retention of records
* maintain the minimum set of records required for undertaking our public functions
* minimise retention costs
* improve operational efficiency; and
* where appropriate, ensure that an adequate historical archive is maintained.

The importance of complying with this policy cannot be overstated. Not only does poor record management have implications for our internal workings, but the external ramifications can be significant. As a Scottish public authority, poor records management will have consequential implications for our ability to comply with our responsibilities under the FOISA, EISR, UK GDPR and DPA.

## CREATING AND DISCLOSING INFORMATION

Every time information is captured in a record it carries with it a degree of risk. This risk exists because of the extensive disclosure obligations to which we are subject, for example our obligations under FOISA. There are numerous examples of seemingly insignificant records (such as handwritten notes made on recruitment records and emails containing "off-the-cuff" comments about ongoing matters) that cause significant problems for organisations and for the staff who made them when they are required to be disclosed in response to a FOISA request. Equally, not being able to respond comprehensively to a FOISA request or from the courts or UK authorities may result in adverse consequences for WICS.

The disclosure obligations to which we are subject may arise in many different contexts:

* As a Scottish public authority, we may be required to disclose information under FOISA, EISRs, UK GDPR or DPA as outlined previously
* Any record required by law to be retained for a statutory or regulatory purpose is also impliedly required by law to be disclosed for that purpose
* In the context of litigation there is a duty on both parties to make full disclosure to the courts, even of records that may adversely affect their case
* Various UK regulatory authorities (such as Her Majesty’s Revenue and Customs) can, in the exercise of their regulatory functions, require us to disclose certain records to them as part of their investigations and general enquiries.

There are some rules that restrict access to records in the above disclosure situations. In a DPA/UK GDPR, FOISA or EISRs context, certain exemptions may be applied, where necessary, to for example protect privacy rights, confidentiality or commercially sensitive information. These regimes are complex and vary in their application on a case-by-case basis. For further information please speak to the Information Manager or DPO.

Once a record is created, it is vitally important not to destroy it if there are concerns about the effect of its disclosure. In the context of dealing with a request for information, the random destruction of or failure to retain records will only invite an adverse inference and may constitute a criminal offence. In such instances the individual employee and the organisation may be found guilty.

## RETENTION OF RECORDS

Certain records should never be destroyed (such as board minutes), and other records must be kept for a specified minimum period by certain specific statutory and regulatory provisions.

The tables set out in appendix 1 to this policy contain details of specific types of records and the retention times that apply to them by specific statutory or regulatory provisions or because of our policy or practice.

Records may be required as evidence in legal proceedings in the future. Depending on the nature of the claim giving rise to the legal proceedings the law provides for certain time limits, or limitation periods, within which claims can be made.

If any applicable specific statutory or regulatory retention periods have been observed in relation to a set of records, those records can then lawfully be destroyed.

We have set out below some of the factors you should consider when deciding which records to keep and which to destroy once any specific statutory or regulatory retention periods have been observed, but before any relevant limitation periods have expired:

* What are the future circumstances in which the records may be required?
* What services do the records relate to?
* Are there any continuing obligations to or on WICS that could be breached in the future?
* How likely is it that a claim could be raised by or against WICS in the future in relation to a matter associated with those records?
* What are the consequences if the records are not available?

The DPA and UK GDPR require that personal information should be kept no longer than is necessary for the purpose for which it was collected. This means that once any applicable statutory or regulatory retention periods have lapsed and limitation periods have been considered, records containing personal information should be considered for destruction on a case-by-case basis. For further information please speak to the Information Manager or DPO.

## STORAGE OF RECORDS

Records may be held in a variety of forms including USB memory sticks, CDs, DVDs, hard disk drives on computers and servers.

The DPA and UK GDPR require appropriate technical and organisational measures to be taken against accidental loss or destruction of or damage to personal information. In other words, records that contain personal information must be kept secure.

Notwithstanding the requirements of the DPA and UK GDPR, security is vital to protect the confidentiality, integrity and availability of all our records. Access to records should be restricted to those people who require it for a specific purpose.

All records on electronic media should be held in a format that is either software independent or the software itself should be retained to ensure that the records are readable. This may involve keeping obsolete software and hardware in working condition and clearly documenting the file formats. However, we are not expected to incur unnecessary expenditure in maintaining such facilities and may consider converting the records into a modern format for easier retention and access, if possible.

A comprehensive record should be kept of where records are stored. This should include details of the period they are to be kept and the procedure for their destruction. This information is contained within our business classification and retention schedule.

One of the main difficulties with electronic storage can be ensuring and proving the integrity of the data. As a rule, computer generated records and copies of paper records generated by a computer process will be admissible as evidence. However, stringent conditions usually must be followed to make them admissible, such as being able to provide a detailed audit trail, outlining the full life cycle of a document from its scan to the system to its subsequent use.

## RETRIEVING RECORDS

When records are required for disclosure for any purpose, the requirement will usually only relate to records that address a specific event or issue. It is therefore important to consider the extent to which records can be retrieved and the searchability of the storage medium on which the records are to be stored. When records need to be retrieved for litigation or at the request of the authorities, there is often only limited time available. As such it is vitally important that we maintain an audit trail of where our records are. We must also ensure that before we send records to storage, they are reviewed to ensure that we have a record of what is being sent and where.

WICS uses a range of IT systems and services to support its data processing and storage requirements. Should there be a requirement to retrieve records from operational systems, it should typically be possible to do so within 48 hours. If there is a requirement to retrieve records from an archive, the recovery time could take longer.

## DESTROYING RECORDS

If we receive a FOISA, EISRs or DPA/UK GDPR request and the routine and planned destruction of records means that we cannot respond fully or at all to such a request, then provided we can demonstrate that the records were destroyed in line with our record retention policy, we should not face any adverse consequences and the risks of commission of a criminal offence are significantly mitigated.

If any litigation, dispute or investigation occurs, then the destruction of records associated with such request, litigation, dispute or investigation should be automatically suspended and steps taken to ensure their preservation.

Any destruction, disposal, falsification, or concealment of such records may result in:

* A Decision Notice and/or an Enforcement Notice being issued by the Scottish Information Commissioner or of the Information Commissioner against WICS
* The claim or defence being struck out
* Serious costs consequences
* The parties or their advisers being held in contempt of court
* The parties or their advisers being found guilty of obstructing or perverting the course of justice; and
* Fines and/or imprisonment for WICS and our employees who are involved.

Any destruction of records, regardless of the media on which they are recorded, must be conducted in a secure manner to ensure that there are safeguards against accidental loss or disclosure during the process of destruction. The destruction of records is an irreversible act. The main methods of destruction are as follows:

* **Salvage disposal and recycling by specialised firms.** The security of each firm’s methods should be fully investigated and guarantees built into any contract, including indemnities in the event of data loss.
* **Shredding.** Shredding undertaken by shredding firms should be supervised by an appropriate member of staff and an appropriate destruction certificate obtained.
* **Erasing electronic data.** Care needs to be taken to ensure that sensitive data is **completely** erased. For example, deleting a file on a PC may only delete the file reference and not the underlying data. With the right tools and knowledge, it is possible to reconstruct the file.

Staff are responsible for managing their own “live” records and must do so in accordance with this policy. As part of this management, it will be for staff to ensure that records are not destroyed prior to the end of the retention period which relates to them, and furthermore to ensure that if destroyed, they are only destroyed in accordance with this policy.

There are important exceptions to these rules. In terms of records that WICS is legally required to retain for a longer period than the default periods set out above, these are highlighted in appendix 1. In addition, if you believe that any of your own records need to be retained for longer periods of time, you should raise this with the Records Manager or DPO. If records relate to a transaction which may carry a significant litigation risk, these should be distinguished from your other records.

## MONITORING AND REVIEW

This policy should be reviewed at least annually, or whenever there are changes in any applicable legislation or regulations. This review process will ensure that account is taken of any new commercial practices, new methods of storage, or changes in the law and that the policy continues to meet our needs.

Compliance with this policy will be reviewed periodically by the Audit and Risk Committee and the WICS Board. Failure to comply will be taken very seriously.

# RECORDS MANAGEMENT DEFINITIONS

Throughout the Information Management Policy, the following terms are used:

"**Controller**" a person who is responsible for determining the purposes and means of the Processing of Personal Data.

"**Data Protection Legislation**" the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) and any other legislation relating to the processing of Personal Data.

"**Data Protection Principles**" the restrictions set down in the UK GDPR relating to the Processing of Personal Data.

"**Data Subject**" the identified or identifiable living individual to whom Personal Data relates.

"**Information Commissioner**" the appointed official responsible for ensuring compliance with DPA.

"**Information Commissioner's Office**" (the "**ICO**") the supervisory authority in the UK responsible for enforcing and monitoring compliance with the DPL and for whom the Information Commissioner is the accountable officer.

"**Personal Data**" information relating to a Data Subject.

"**Processing**" any operation performed on Personal Data, whether or not by automated means, including 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.

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

"**Special** **Category Personal Data**" Personal Data relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, sexual life or sexual orientation; or genetic or biometric data where processed for the purpose of uniquely identifying a Data Subject.

# APPENDIX 1: RECORD TYPES AND RETENTION PERIODS

PROCUREMENT

Information Asset Owner: Head of Finance

|  |  |  |  |
| --- | --- | --- | --- |
| Record type | Retention period | Retention method | Reasons |
| A record in relation to each public contract awarded by WICS or framework agreement concluded by it. | No period specified in relevant legislation.  Three years from date of contract award for unsuccessful  Six years from end of contract for successful. | Electronic or hard copy | Limitation period for bringing claims and Regulation 83(9) of the Public Contracts (Scotland) Regulations 2015. |
| A record of progress of contract award procedures. | No period specified in the relevant legislation.  Three years from date of contract award for unsuccessful  Six years from end of contract for successful. | Electronic or hard copy | Limitation period for bringing claims and Regulation 83(9) of the Public Contracts (Scotland) Regulations 2015. |

PROPERTY

Information Asset Owner: Director of Corporate and International Affairs

|  |  |  |  |
| --- | --- | --- | --- |
| Record type | Retention period | Retention method | Reasons |
| Building contracts, collateral warranties, appointments etc | Until later of:   * WICS disposing of interest in the property and * expiry of any agreed limitation period in contract. | Hard copy with electronic back-up | Limitation period for bringing claims |
| Inspection reports e.g. boilers, operating manuals | Until item replaced. | Electronic or hard copy | Best practice recommendation |
| Health and safety file | Three years after WICS ceases to have an interest in the property. | Hard copy with electronic back-up | Health & Safety Regulations and limitation period for bringing claims |
| Product or Treatment Guarantees | Until later of:   * WICS disposing of interest in the property and * expiry of any agreed limitation period in guarantee. | Hard copy with electronic back-up | Best practice recommendation |
| Title deeds / leases | As long as WICS have an interest in the property. | Hard copy with electronic back-up | Best practice recommendation |
| Missives | Until date of supersession in terms of missives. | Hard copy with electronic back-up | Best practice recommendation |
| Building Insurance | Permanently. | Electronic or hard copy | Best practice recommendation |
| Planning and Building Warrant documentation | Five years following WICS ceasing to have an interest in the property. | Hard copy with electronic back-up | Planning and Building Control Regulations |
| Environmental health reports | Until later of:   * WICS disposing of interest in the property and * superseded by subsequent reports. | Electronic or hard copy | Best practice recommendation |
| VAT / Transfer of going concern documentation | Six years from end of accounting period to which they relate. | Hard copy with electronic back-up | VAT Regulations |
| Fire risk assessment | Permanently. | Electronic or hard copy | Fire Regulations |
| Ground condition reports | Five years following WICS ceasing to have an interest in the property. | Electronic or hard copy | Best practice recommendations |
| Details of capital allowances claimed | Six years from end of accounting period to which they relate. | Electronic or hard copy | Capital Allowances Regulations |

ADVERTISEMENT AND RECRUITMENT RECORDS

Information Asset Owner: Director of Price Review

|  |  |  |  |
| --- | --- | --- | --- |
| Record Type | Retention period | Retention method | Reasons |
| Job adverts, application packs (information given out by WICS) | One year from date of last appointment to the vacancy. | Electronic or hard copy | Best practice recommendation |
| Application forms, interview notes, reference requests, criminal convictions | Six months for unsuccessful applicants  Six years post termination of employment for successful applicants.  If the applicant has been recruited and now works for WICS, delete information that is not relevant to ongoing employment. | Electronic or hard copy | The Information Commissioner's Employment Practices Code and the discrimination statutes. |

Employment Records

Information Asset Owner: Director of Corporate and International Affairs

|  |  |  |  |
| --- | --- | --- | --- |
| Record Type | Retention Period | Retention Method | Reasons |
| Grievances and associated documentation | Date of termination of contract of employment + six years | Electronic or hard copy | Discrimination statutes and best practice recommendation |
| Working time opt-out records and compliance records | Two years from date on which records were made | Electronic or hard copy | Working Time Regulations 1998 |

Absence, health and accident records

Information Asset Owner: Director of Corporate and International Affairs

|  |  |  |  |
| --- | --- | --- | --- |
| Record type | Retention period | Retention method | Reasons |
| Written statement of policy with respect to health and safety at work and WICS arrangements for carrying out that policy. | Permanent.  All employers must have policy in place and bring the statement and any revision of it to the notice of all employees. | “Written statement” is required but an electronic or hard copy will suffice | Health and Safety at Work Act 1974 |
| Sickness records where major injuries were received at work. | 40 years from date of termination of contract of employment. | Electronic or hard copy | Limitation period for bringing claims |
| Records made following health and safety risk assessment and subsequent measures put in place to prevent hazards and protect employees. | 40 years from date of undertaking assessment | Electronic or hard copy | Limitation period for bringing claims |
| Records relating to disability where employee has a disability as defined by the Equality Act 2010. | Six months from date of termination of employment. | Electronic or hard copy | Limitation period for bringing claims and best practice recommendation |

Statutory leave and flexible working requests

Information Asset Owner: Director of Corporate and International Affairs

|  |  |  |  |
| --- | --- | --- | --- |
| Record type | Retention period | Retention method | Reasons |
| Any request to work flexibly | Duration of employment + six months post termination. | Electronic or hard copy | Employment Rights Act 1996 and limitation period for bringing claims. |
| Requests for parental leave and associated documentation. | Duration of employment + six months post termination of employment. | Electronic or hard copy | Maternity and Parental Leave Regulations 1999 and limitation period for bringing claims. |
| Requests for paternity / adoption leave and associated documentation. | Duration of employment + six months post termination | Electronic or hard copy | Paternity and Adoption Leave Regulations 2002 and limitation period for bringing claims. |

Wages, payments and tax records

Information Asset Owner: Head of Finance

|  |  |  |  |
| --- | --- | --- | --- |
| Record type | Retention period | Retention method | REASONS |
| PAYE records (not including those that must be sent to HMRC). | Three years after the end of the financial year to which the records relate. | As required by HMRC | The Income Tax (Pay As You Earn) Regulations 2003 |
| Income tax and NI returns, including correspondence with tax office. | Three years after the end of the financial year to which the records relate. | As required by HMRC | Income Tax (Pay As You Earn) Regulations 2003 |
| Statutory maternity, paternity and adoption pay records and calculations. | Three years after the end of the financial year to which the records relate. | As required by HMRC | Statutory Maternity Pay (General) Regulations 1986 and  Statutory Paternity Pay / Statutory Adoption Pay (Administration) Regulations 2002. |
| Statutory Sick Pay records and calculations. | Three months after the end of the period of sick leave to which they relate or  6 years post termination of employment. | As required by HMRC |  |
| Wages / salary records (including details of benefits, expenses and bonuses). | Six years from end of period for which WICS may be required to deliver a tax return | As required by HMRC | Taxes Management Act 1970 Prescription and Limitation (Scotland) Act 1973 |
| National Minimum Wage compliance records. | Three years beginning on the date upon which the pay reference period immediately following that to which the records relate ends. | As required by HMRC | National Minimum Wage Regulations 2015 |

Disclosure of Information

Information Asset Owner: Director of Corporate and International Affairs

|  |  |  |  |
| --- | --- | --- | --- |
| Record type | Retention period | Retention method | Reasons |
| Information disclosed to trade unions. | No specified time but at least until act to which information is disclosed has happened. | Electronic or hard copy | Best practice recommendation |
| Information disclosed to employees / employee representatives in relation to TUPE transfers. | Three months from date of completion of transfer. | Electronic or hard copy | TUPE Regulations 2006 and limitation period for bringing claims |

Redundancy Information

Information Asset Owner: Head of Finance

|  |  |  |  |
| --- | --- | --- | --- |
| Record type | Retention period | Retention method | Reasons |
| All documentation relating to redundancies where more than 20 employees affected | Five years from date of last redundancy unless proceedings outstanding. | Electronic or hard copy | Trade Union and Labour Relations (Consolidation Act 1992) Sections 193-194 |

Miscellaneous Information

Information Asset Owner: Director of Corporate and International Affairs

|  |  |  |  |
| --- | --- | --- | --- |
| Record type | Retention period | Retention method | Reasons |
| Anonymised statistical information being kept for analysis e.g. exit interviews, equal opportunities monitoring etc. | Either a period agreed with the person who is the subject of the information (if not anonymised), or no longer than is necessary for the purposes of analysis of the information (if it is anonymised). | Electronic or hard copy | Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 and related Codes of Practice |
| Correspondence with government agencies in relation to employees (e.g.  Child Support Agency, Family Credit) | Duration of employment | Electronic or hard copy | Best practice recommendation |
| Certificate of Employers' Liability Insurance Cover | Permanent | Electronic or hard copy | Best practice recommendation |
| Personal information of any sort on a web page/site | No longer than a period specifically agreed with individual. | Electronic or hard copy | Best practice recommendation |
| Outlook mailbox items including emails, folders and calendar entries. | If tagged by mailbox owner, item retained for maximum of 6 years from receipt, unless manually deleted before then. If not tagged, item will be retained for maximum of 6 months from receipt, unless manually deleted before then.  Items deleted manually or automatically are retained for an additional maximum 30 days in the mailbox deleted items.  Items that are deleted manually or automatically from deleted items folder are further retained for maximum of 14 days unless purged from “recover deleted items”. | Electronic copy | Best practice recommendation |

|  |  |  |  |
| --- | --- | --- | --- |
| Temporary workers and self-employed workers | | | |
| Information Asset Owner: Director of Price Review | | | |
| Record Type | Retention Period | Retention Method | Reasons |
| All documents as listed above (sections 3.1-3.9) relating to temporary workers on placement for less than a year. | Six months from date of termination of placement | Electronic or hard copy | Discrimination statutes. |

Duties as a non-departmental public body

Information Asset Owner: Head of Finance

This table relates to WICS' statutory duties, as established under the Water Industry etc. (Scotland) Act 2005, under the sectoral legislation only. The minimum retention period in relation to the information required to be kept under the sectoral legislation may be different than that under legal requirements covered elsewhere in this policy. Where the same information is to be retained under other legal requirements, WICS should comply with the longer of the retention periods.

|  |  |  |  |
| --- | --- | --- | --- |
| Record type | Retention period | Retention method | Reasons |
| Register of gifts and hospitality | Duration of appointment | Electronic or hard copy | The *Ethical Standards in Public Life (Scotland) Act 2000* ("2000 Act") |
| Register of interests | Five years after date member ceases to be a member | Electronic or hard copy | *Ethical Standards in Public Life (Scotland) Act 2000 (Register of Interests) Regulations ("*the 2000 Regulations"*).* |
| Annual report and financial statements | There is no statutory requirement to retain the information used to produce the Annual Report or the Annual Report itself after it has been superseded. However, as a matter of good practice WICS should archive its Annual Reports. | The document must be published. Electronic or hard copy | Section 6 of the 2000 Act requires the production and publishing of an Annual Report.  Paragraph 14 of Schedule A1 of the 2000 Act required the production of Annual Accounts. |
| Pension scheme documentation | No statutory retention period. Documents should be kept for at least the lifetime of the scheme. | Original hard copy signed versions, where applicable. Otherwise, electronic or hard copy. | To deal with any queries/claims relating to scheme and requests under disclosure of information laws.  To allow regular review of the Statement of Policy to ensure it reflects any changes in WICS discretionary policy and the LGPS governing regulations. |
| Information Asset Owner: Director of Price Review | | | |
| Record type | Retention period | Retention method | Reasons |
| Register of Licences | There is no particular period specified, but this should be at least for the life of licensing regime. | Electronic or hard copy | Paragraph 12 of Schedule 2 to the Water Services etc. (Scotland) Act 2005 ("2005 Act") |
| Industry documentation: Fees scheme, disconnections code, Section 29E departure procedure | No particular time period however copies of these documents should be retained for an indefinite period. Where revised or superseded, the historic versions should also be retained in case an issue arises that was governed by the previous version of the document. | Electronic or hard copy or both. | Water Industry (Scotland) Act 2002, 2005, 1980  Sewerage (Scotland) Act 1968 |