Llywodraeth Cymru
Welsh Government

WELSH GOVERNMENT

INFORMATION MANAGEMENT AND GOVERNANCE POLICY

PUBLISHED: AUGUST 2018

LAST REVIEWED: FEBRUARY 2019

Contacts: Name Redacted @gov.wales)
Name Redacted @gov.wales)
Discovery & Appraisal Unit – I&S

Policy Owner: Permanent Secretary

Description: This policy defines the way Welsh Government information and records should be managed to standards which ensure that vital and important records are identified, that the Welsh Government holds records that are necessary, sufficient, timely, reliable and consistent with operational need, and that legal and regulatory obligations are met. It also defines the roles and responsibilities for the creation, safekeeping, assurance, use, re-use, storing, sharing, publishing and disposition of information.

Publication: This policy is located on the Welsh Government Intranet and on

our website

This policy replaces the Welsh Government Information and Records Management Policy of May 2015

Welsh Government Information Management and Governance Policy

The Permanent Secretary and her Senior Team recognise information management as a specific core corporate function and ensure the necessary levels of organisational support to enable its effectiveness. The programme brings together responsibilities for information, data and records as corporate assets, in all formats, throughout their life cycle from creation or receipt through to disposal (destruction or archiving).

To comply with the Public Records Act 1958 and other information management legislation, the Welsh Government needs to know what information it possesses, how old it is and to ensure that it constitutes reliable evidence. For sensitive information, including that covered by the General Data Protection Regulation (GDPR) (EU) 2016/679, the Data Protection Act 2018 & Law Enforcement Directive (LED) 2018, we must be able to allow access to those who need to see this information while preventing others from gaining access. We also need to be able to identify personal information, know who it is shared with, and dispose of information we are no longer entitled to hold.

SUMMARY STATEMENT

This policy statement sets out the commitment of the Welsh Government to manage information in a professional manner, to ensure that its information base is efficiently exploited, whilst providing accountability and assurance. It is supported by a framework of more detailed data, information and records, and security policies.

The Welsh Government uses an eight stage Information Lifecycle: Create, Assure, Use, Store, Access, Share, Publish and Dispose.

Create

The policy defines how the Welsh Government applies good information management principles to information (data, documents or records) created or received as part of its activities.

Our policy is to:

- assign a meaningful title in a consistent format to all information, so that its content is clear and it indicates when a file contains personal data
- ensure the correct retention (Information Type) is applied at creation
- apply version control (documents created and stored on systems other than our corporate EDRMS, iShare) so the latest version can be easily identified, and whether it is a draft or published version
- apply sufficient metadata to aid retrieval and to provide context ('who', 'when', 'why' etc.)
- label information with appropriate protective markings, in accordance with current Security policy and guidance.

Assure

The policy defines how the Welsh Government assures information (including personal information), and the systems and processes used, so that it is appropriately protected whilst also being fully utilised for maximum benefit to the organisation.

Our policy is to:

- assess and manage risks to the confidentiality, integrity and availability of information throughout the information lifecycle
- balance the need to protect information with the need to effectively make use of it
- develop a risk-aware culture
- take measures to protect information from inadvertent or unauthorised access, alteration, transmission or destruction
- comply with legislative and mandatory requirements relating to the protection or destruction of information
- appoint appropriately qualified individuals to roles with clearly defined responsibilities for information assurance
- ensure the privacy of users and protect personal data
- ensure we have the powers and a valid lawful basis to process personal data
- maintain Information Asset Registers (IARs)
- ensure that contracts, grants, Memorandums of Understanding (MOUs) and other third party arrangements are up to date and properly cover any processing of personal data
- ensure that all privacy notices are up to date
- undertake appropriate Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments
- ensure privacy by design[1] when undertaking ICT procurements
- report information security incidents (including data breaches) to the Departmental Security Unit (DSU) as soon as we are aware of them and where appropriate notify the Information Commissioner within 72 hours
- ensure that all staff are aware of their responsibilities regarding information, its management and use

Our SIRO Risk Appetite Statement defines at a practical level how the Welsh Government protects its information assets. Our Information Security policy sets out the approach to ensure our information assets are properly protected against a variety of threats (such as error, fraud, sabotage, terrorism etc.).

Use

The policy defines how the Welsh Government uses systems (including manual systems) to create, store or process information, taking account of privacy and sensitivity requirements and statutory obligations.

Our policy is to:

- manage the systems used to create, store or process information as corporate resources

[1] Privacy by Design holds that organisations need to consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data.

- fully exploit information and systems by sharing, reusing and repurposing wherever possible and appropriate
- consider privacy and sensitivity issues when using information and systems, and comply with mandatory requirements and statutory limitations
- ensure all staff are aware of their responsibilities for the management and use of information and systems
- where necessary implement appropriate technical controls (including monitoring)
- ensure that the necessary authority to process, collect, and share personal data are in place
- ensure the transparency of government data, making this available for re-use by third parties (including the public) by publishing in reusable form
- use licensing arrangements, in accordance with Public Sector Information regulations, to encourage the re-use of government data

Store

The policy defines how and where the Welsh Government stores business information to maximise efficiency, reduce costs, enable sharing, and minimise risks.

Our policy is to:

- correctly store information, regardless of format / medium, on an approved system (e.g. iShare, CaSSi and IRIS) using a recognised file plan
- store personal data in an appropriate area with the right authorisations and access controls
- store physical information in registered files, but only when it is impossible to create a valid electronic version
- not store information permanently on removable media (e.g. CD-ROM, DVD) as these may degrade over time and are less secure
- not store business information in formats which are likely to be unsupportable long-term, and migrate information when formats do change
- restrict the size of “individual” storage areas, iShare personal home areas, desktop areas and Outlook mailboxes so that they are sufficient for short term use
- apply and maintain a corporate Retention Schedule
- store information on accredited systems or in areas appropriate to the protective marking
- minimise the amount of personal data required and only keep that which is absolutely necessary
- do not keep contact lists beyond the stated retention period, or use them for anything other than their original purpose.

Access

The policy defines how Welsh Government information is to be made accessible to all those with a business need to see it, both internally and externally. Information will remain accessible and findable for as long as it is needed, and will be preserved permanently where appropriate.

Our policy is to:

- only limit access to information when necessary due to security, privacy or sensitivity requirements

- apply access controls to protect information, including personal information, which should not be generally accessible
- use a corporate taxonomy to index documents for improved retrieval by search engines
- identify information which is vital to essential core functions, which must be restored promptly in the event of a disaster
- check that information is presented in compliance with the Disability Discrimination Act

Share

The policy defines how the Welsh Government shares information (internally, with third parties and with the public) to ensure it is available for re-use, to encourage openness, and to comply with legal requirements (e.g. Freedom of Information Act 2000, the General Data Protection Regulation (GDPR), Data Protection Act 2018, Environmental Information Regulations, Re-use of Public Sector Information Regulations 2015, and Copyright Act 1988).

Our policy is to:

- manage all business information as a shared resource within the Welsh Government, with access only limited when there are security, privacy or sensitivity requirements.
- send iShare links internally rather than reproducing or sending attachments in emails
- where possible, use iShare Connect, Egress, etc. when sharing information with colleagues outside the Welsh Government
- ensure that documents shared with third parties do not contain comments, tracked changes, or similar 'hidden' content. In the rare circumstances where documents with comments are to be shared, permission from the relevant IAO must be obtained
- recognise and protect Intellectual Property Rights when appropriate
- comply with the statutory access provisions of the Freedom of Information Act, the GDPR, Data Protection Act 2018, Environmental Information Regulations (EIR)and Public Sector Information Regulations (RPSI)
- proactively make information available to the public in accordance with the Welsh Government publication scheme
- share only the minimum of personal data required to meet business purposes, and do so in a secure manner compliant with relevant legislation

Publish

The policy defines how the Welsh Government publishes information externally, ensures it is of appropriate quality in terms of content and format, and complies with appropriate standards.

Our policy is to:

- apply a formal review and approval process to information published externally to ensure content does not breach security or sensitivity
- apply copyright statements to all publications
- recognise and protect Intellectual Property Rights

- allocate an ISBN (International Standard Book Number) or ISSN (International Standard Serial Number) as appropriate, to all publications
- use appropriate re-use statements including the Open Government Licence (OGL)
- proactively make information available for third party re-use by publishing in reusable forms and under enabling licensing conditions (in accordance with RPSI)
- comply with legal deposit legislation by providing a copy of all works published (in whatever format) to the British Library and the National Library of Wales within a month of publication
- apply corporate identity standards to all publications.

Dispose

The policy defines how the Welsh Government disposes of its information. Disposal is the final stage of the Information Lifecycle when information is given a further review date, transferred to The National Archives for permanent preservation, or destroyed.

Our policy is to:

- consider the 'whole-of-life' disposition of information at the time of its creation
- only retain information for as long as there is a business or regulatory need, and protect still-sensitive information.
- delete personal information that is no longer required in accordance with the retention statement in the relevant privacy notice
- apply retention and disposal schedules to all information held in shared corporate repositories
- comply with the requirements of the Public Records Act and Freedom of Information Act Section 46
- destroy information securely so that reconstruction or recovery is unlikely.

This policy is effective from: ......21....August......2018...
(date of signature)

Signed: ..... **Personal Data** ....

Shan Morgan

Permanent Secretary

Welsh Government

WELSH GOVERNMENT INFORMATION MANAGEMENT AND GOVERNANCE POLICY

Contents

Background

The Permanent Secretary and her Senior Team recognise information management as a specific core corporate function and ensure the necessary levels of organisational support to enable its effectiveness. The programme brings together responsibilities for information, data and records as corporate assets, in all formats, throughout their life cycle from creation or receipt through to disposal (destruction or archiving).

To comply with the Public Records Act 1958 and other information management legislation, the Welsh Government needs to know what information it possesses, how old it is and to ensure that it constitutes reliable evidence. For sensitive information, including that covered by the General Data Protection Regulation (GDPR) (EU) 2016/679, the Data Protection Act 2018 & Law Enforcement Directive (LED) 2018, we must be able to allow access to those who need to see this information while preventing others from gaining access. We also need to be able to identify personal information, know who it is shared with, and dispose of information we are no longer entitled to hold.

This policy applies to all personnel carrying out work on behalf of Welsh Government. This includes permanent and temporary employees, secondees, consultants, suppliers, partners, contractors and subcontractors.

1 Why do we need an Information Management and Governance Policy?

The Civil Service Code requires that Welsh Government staff "keep accurate official records and handle information as openly as possible within the legal framework"[2].

Freedom of Information and Data Protection legislation put great emphasis on the Welsh Government's ability to make information available to the public, as well as appropriate processing of personal and sensitive personal data. These legislative obligations highlight the need for an effective framework for information and records management to be in place throughout the organisation as a mechanism for managing and retrieving information on demand and ensuring the appropriate processing of personal and sensitive personal data.

The key pieces of legislation are:

- Public Records Act 1958 & 1967
- Government of Wales Act 1998 & 2006
- General Data Protection Regulation (GDPR) (EU) 2016/679
- Data Protection Act 2018
- Law Enforcement Directive (LED) 2018

[2] The Civil Service Code applies to all home civil servants who are members of staff of the Welsh Government.
http://wales.gov.uk/about/recruitment/currentvacancies/generalappointments/civilservicecode/?lang=en

- Freedom of Information Act 2000 - including the Lord Chancellor's Code of Practice on the Management of Records issued under Section 46
- Environmental Information Regulations 2004 (EIR)
- European Directive on the Re-use of Public Sector Information 2003 and the
- Protection of Freedoms Act 2012 (Part 6 Section 102)
- Constitutional Reform and Governance Act 2010 (Part 6 Sections 45 & 46)
- Copyright, Designs and Patents Act 1988
- The Re-use of Public Sector Information Regulations 2015
- CCTV Code of Practice (ICO)

Managing this information to agreed standards as it is created is essential if those records are to be understood or used in the future. The availability, re-usability and life of the information or record depend on it being managed according to its context and value.

Information and records are also needed to provide an audit trail of evidence. As well as forming evidence of the transactions we undertake, many records actually define the boundaries within which these transactions must occur and dictate the way in which they are carried out. Important decisions are taken against the contents of these records as they exist at the time. It is therefore vital to be able to pin-point exactly what the record said at any given point in time in order to verify the validity of the decisions made.

Records and information are also kept to maintain the corporate memory. It is essential that Welsh Government officials have timely access to the records created by their predecessors in order to deliver evidence based policy making.

The ISO standards and requirements for electronic records management can be found here.

2 What is the Aim of our Information Management and Governance Policy?

The aim of the policy is to ensure that all parties are aware of their personal obligations regarding the efficient, cost effective and legally compliant creation and management of information and records. This document explains Welsh Government's Information Management principles (policy statement).

Information and records created by all personnel remain the property of Welsh Government under the terms of Crown Copyright. Re-use of Government information is outlined in the Re-use of Public Sector Information Regulations 2015.

3 What is the Scope of our Information Management and Governance Policy?

The scope of this policy is all information and records created during the delivery of the Welsh Government's objectives.

4 What constitutes Welsh Government Information & Records?

The ISO standard, ISO 15489-1:2016 Information and documentation - Records management[3] defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations[4] or in the transaction of business'. It applies to the creation, capture and management of information and records regardless of structure or form, in all types of business and technological environments, over time.

This policy relates to information created and held in all formats and media including, but not limited to, the following:

- Documents, presentations and spreadsheets received and stored digitally
- Paper based files
- Social media, wikis and blogs
- Emails
- Diaries
- Faxes
- Brochures and reports
- Welsh Government pages on both the intranet and the external internet
- Forms
- Evidence supplied by third parties
- Information created by third parties on our behalf
- Mobile tools (e.g. iPhones)
- Audio and video recordings
- Maps and plans
- Images & photographs
- Microfiche and microfilm
- Websites
- Text messages, instant messaging, etc.

The Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 applies to all records irrespective of media or the type of information they contain. Welsh Government business areas have to ensure that these systems and the records they hold are managed in compliance with the Code. These systems must be listed in the Welsh Government's Information Asset Register and meet corporate records management and security requirements (access, retention / disposal, preservation etc.). Records held on these systems with long term business value should be migrated to iShare for long term preservation.

[3] https://www.iso.org/standard/62542.html

[4] The Welsh Government's "Public Task" - http://gov.wales/about/foi/policies/public-task-statement/?lang=en

5 Are there any related Welsh Government Policies and Guidance?

- Welsh Government Code of Practice on Access to Information
- Welsh Government Security Policy
- Welsh Government Information & Security Policy
- Backup policy
- Social Media Strategy
- Procurement Checklist
- Private Office Guidance
- SIRO Risk Appetite Statement
- Open Data Plan
- Data Breaches and 'Near-Misses'
- Privacy Impact Assessment (PIA)
- Equality Impact Assessments (EIA)
- Instant Messaging Policy

6 What are our Corporate Information Management Systems?

6.1 Hardware & IT equipment (Laptops, iPads, iPhones, etc.)

You will be provided with Welsh Government IT equipment. The equipment will be connected to the Welsh Government network servers with access to the internet, email and iShare. If you require additional software for a specific purpose, please discuss this with your line manager.

You are responsible for the security and safety of the hardware and any information created and stored on these systems.

6.2 Approved Corporate Information Management Systems & Software

The following systems are approved for the storage of corporate records and information. They may be used to store OFFICIAL and OFFICIAL-SENSITIVE information. SECRET and TOP SECRET information should be stored in accordance with the Information Security Policy.

Exceptionally, there may be justification for holding records on a network drive location.

System	Definition
iShare (Electronic Document and Records Management System – EDRMS)	iShare rollout was officially completed in March 2012. It is the corporate repository for the majority of information created and received by Welsh Government officials in the course of their duties that must be retained for business or historical purposes.

System	Definition
Shared Drives	It is not technically feasible to store certain types of linked spreadsheets and databases in iShare. There are also software packages which do not natively integrate with iShare. These are stored on teams' shared drives. There must be a pointer from iShare to these repositories. It is the responsibility of the teams concerned to organise the content on these shared drives using the Retention and Disposal Schedule. The shared drive (R:drive) is limited to the following: • complex interlinked spreadsheets which are not compatible with iShare. iShare provides a level of compatibility with interlinked spreadsheets and advice should be sought from Information and Records Management on compatibility. • Active Access databases which should not be stored in iShare. Non-active Access databases and periodic snapshots of Access databases should be stored in iShare. The shared drive (S: drive) is limited to the following: • temporary storage for software which does not directly integrate with iShare. The information should be manually added to iShare and removed from the drive at the earliest opportunity. • storage of video files until such time that a more suitable solution can be found. The S: drive is limited by size and teams must manually move information to iShare as soon as possible.
HR Self Service (previously "Snowdrop")	Human Resources management software – for HR administration e.g. annual leave and sickness absence
SAP Finance System	The Welsh Government corporate financial management system.
PPIMS	WEFO's Project and Programme Information Management System (PPIMS). PPIMS holds records of all projects that have received a verification visit, holding the necessary data for the EU Commission

System	Definition
CaSSI	An integrated, customer focused self-service IT system for Care Inspectorate Wales (CIW). The CaSSI system stores information in iShare using application level integration which is invisible to the user.
EDDMS	An ICT system to manage roads projects within Transport: wag.causeway.com
IRIS	An integrated, customer focused self-service IT system for Cafcass Cymru. The Cafcass Cymru CRM system stores information in iShare using application level integration which is invisible to the user. The database also contains information about the service users, court hearings etc.

6.3 Other Systems

The following systems are in use but are not Corporate Information Management Systems:

System	Definition
iShare Home Folder	Staff may need to save information which does not form part of the Welsh Government's corporate record and is not appropriate to save within the iShare file plan. For this reason all staff have access to a personal iShare Home folder. Corporate information must not be stored in an individual's iShare home folder.
iShare MyTemp files	A folder to store information temporarily. Any item stored in this folder will automatically delete after 7 days if unused.
iShare Connect	A tool for sharing information within iShare with external stakeholders. The information itself must be stored within registered files in iShare – Connect is not a place to store corporate information. The external Connect web portal should not be used by Welsh Government staff to manage documents - this should be done from within the designated Connect areas in iShare.

System	Definition
MS Outlook	Incoming and outgoing emails of a transitory nature – these should be deleted once actioned and are no longer of immediate business use. If emails form part of a transaction or evidence of business they must be put on record and saved in iShare as soon as possible.

We also hold information in a number of other systems including, but not exclusively:

- Case management systems
- Grant management systems
- Geographical information systems

Information and records held in these systems should be moved to iShare at the earliest opportunity or, where this is not feasible, referenced within iShare registered files.

6.4 Hardcopy

Active hardcopy files accepted as official records are those with SECRET and TOP SECRET security classifications.

Scanning of hardcopy documents received by the Welsh Government, even where they include a signature, is now the accepted procedure but legal guidance should be sought if there is any uncertainty around high risk information. Receipts for T&S claims were previously held on hardcopy "blue files". However, in 2017 the HMRC announced that it would be acceptable for T&S receipts to be held in electronic format instead. Therefore, WG policy is now for original T&S receipts to either be scanned or photographed and saved to the appropriate virtual file on iShare.

With effect from the 1 April 2019 all records relating to Welsh Procurement Card transactions must be retained electronically. Cardholders who do not have access to iShare should where possible make arrangements for a colleague within their directorate to upload the receipts for them. If this is not possible the Card Administrator will in exceptional circumstances arrange for a physical file to be issued. See Annex A.

A small number of hardcopies can be kept in addition to the official record on iShare for reference purposes, as long as security restrictions are followed and the copies are appropriately destroyed when no longer of use (and are not retained beyond the life of the originals). However, staff must not keep complete hardcopy sets of material held on iShare as "back-up". This creates unnecessary additional storage issues / costs and, because they sit outside the official recordkeeping system, they may not be managed appropriately increasing the risk of the WG being in breach of the GDPR, the Data Protection Act 2018 and Section 46 of the Freedom of Information Act.

Recent "yellow files" can be retained on-section for reference. However, those no longer needed for regular consultation should be sent for archiving, via the Information & Records Management team. These records will be stored and retained for the appropriate period (as specified in the Retention & Disposal Schedule) and will then either be destroyed or sent for permanent preservation at the National Archives or other designated Place of Deposit, as appropriate.

6.5 Websites, Social Media and "YouTube"

Welsh Government websites contain public records and are also considered to be of archival value. We archive all websites of the Welsh Government and affiliated bodies in order to provide continued access to key government documents through links persistence. This is also important due to the huge increase in the significance of the web in enabling the Welsh Government to carry out its business. The National Archives has produced an Operational Selection Policy which outlines the requirements for website archiving.

Welsh Government websites are captured, preserved, and made accessible via the UK Web and the UK Government Web Archive. The web archive includes videos, tweets, and websites dating from 2006 to present.

We have a separate Social Media Strategy which sets out rules regarding the acceptable use of social media (e.g. Facebook, blogs, Twitter) within the Welsh Government in a work context and how social media can be used to engage with the public and stakeholders on behalf of the Welsh Government.

6.6 Text & Instant Messaging

Text or 'instant messages' are electronic mail and messaging systems used for the purposes of communication between individuals. Staff should be aware that when using their WG phones in this way they are in fact creating "public records". Staff using private phones for WG business may also be creating public records. The ephemeral nature of text messages (and instant messaging) heightens the need for users to be aware that they may be creating records using this application, and to properly manage and preserve record content.

There are some records management challenges associated with text messages:

- These systems are not designed with a records management functionality, such as the ability to identify, capture, and preserve messages
- The use of multiple electronic messaging systems, types of devices to communicate, and service providers adds complexity to recordkeeping
- Concerns about ownership and control of records created in third-party systems, such as Facebook or Twitter
- Limited search capabilities to manage access and retrieval
- Difficulty in associating messages with individual accounts or case files
- Identification of appropriate retention periods within large volumes of electronic messages
- Capture of complete records, including metadata and any attachments, in a manner that ensures their authenticity and availability
- Development and implementation of records schedules, including the ability to transfer or delete records, apply legal holds on one or several accounts, or perform other records management functions
- Public expectation that all electronic messages are both permanently valuable and immediately accessible.

MicroSoft Teams is part of Office 365 and replaces instant messaging, Skype and Yammer. The contents of chats will be hosted by the Welsh Government and will be retained for 30 days. It therefore comes within the scope of both Freedom of Information and Data Subject requests. **MicroSoft Teams must not be used to make business, finance or policy decisions**.

7 Information Asset Registers (IAR[5])

A list of information assets across the Welsh Government directorates has been compiled in order to achieve and maintain appropriate protection and identify responsibility for groups of assets. Information Asset Owners (IAOs) are responsible for understanding what information is held, what is added and what is removed, how information is moved, and who has access and why.

8 What Information Management measures need to be put in place when using new systems?

In any ICT enabled project, it is essential that all recordkeeping requirements around information created or held within a newly developed and/or implemented system are considered. As well as business needs, this is to ensure that legal and other requirements are met. These will include requirements under the GDPR / Data Protection Act, the Freedom of Information Act and associated Code of Practice on Records Management, Public Records Act 1958, the Statute of Limitation and the Regulatory and Investigatory Powers Act, and will involve:

- Access and security – to ensure that appropriate protection and permissions are set
- Retention and disposal, digital continuity and archiving – to ensure that information is retained for as long as it is needed and then disposed of at the appropriate time
- Audit requirements – particularly where EU funding is involved
- Legal admissibility – to ensure that the information held is acceptable as evidence for audit purposes and in case of inquiry or legal proceedings. This will require compliance with BSI DISC PD0008.

The Information & Records Management Branch will be informed of new project areas via the iPAF process and will enter into discussions with project managers/developers to ensure that the project's information requirements are met.

[5] An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycle.[Cabinet Office definition]

9 What Security Classifications does Welsh Government use?

The Welsh Government adopted the HMG Security Classification Policy for all records created from April 2014.

Historical files retain the classification system that was in place when they were created in order to preserve the administrative history and context of those files.

NB - 'Lock down' or password protection of Word documents. No Welsh Government documents should be locked down or password protected. It restricts the document's ongoing accessibility and readability. Information that requires access restriction or special protection must be filed in an iShare caveated file/folder. Divisions will be responsible for any costs incurred to unlock password protected documents.

10 What is our approach to Naming Conventions?

When creating new records, we use a "Who-What-When" approach to standardise our naming conventions for documents and files:

- Who is the file about (stakeholder, project etc.)
- What is the file about (e.g. meeting papers, Travel & Subsistence etc.)
- When does the file refer to (e.g. 2018, FY2018-2019, 2018-2020 etc.)

The name can contain one or more of the bullet points above and must describe the file sufficiently so that its content is clear. File metadata assists with cataloguing, but the title should be "stand alone".

This is not prescriptive and can be adapted to suit different needs, with the onus on Divisions to agree and adopt a suitable naming convention based on these guidelines. The Information & Records Management team ensure consistency by checking file titles for their suitability whenever a new file is created or when a new project is set up.

11 How do we manage File Closures?

When a project is formally disbanded or when a piece of work has been completed and the files are ready to be closed, staff must contact their file plan managers to officially close the files on iShare. Re-opening of files is not advisable and is only done with the approval of the Information & Records Management team.

For the purposes of Access to Information requests involving project documentation, responsibility for responding to individual requests rests with the owner of the document at the time of the request – i.e. project, programme office or business owner within an inheriting function as appropriate. Duplicate documents and supplementary information of no further use (in all formats) should be deleted / destroyed.

In the case of both stand alone projects and those within programmes, the teams who will provide on-going support or will have on-going policy responsibility must formally accept handover of the relevant information and ensure that the procedure is documented. It is therefore vital that these documents are included as project products at the relevant stages. Prepared handover notes must include a list of all files, their title or subject matter, covering dates, location and security classification, and media format of any duplicates.

All inactive paper records must be archived, via the Information & Records Management team.

12 How do we manage our Email?

It is not appropriate to store emails which constitute an official record in Outlook folders. If emails form part of a transaction or evidence of business they must be put on record and saved in iShare as soon as possible. Emails will be automatically deleted from the Outlook inbox and outbox 12 months after receipt or creation.

It is the sender's responsibility to ensure that emails containing information that must be kept on record are saved into the appropriate file on iShare (or equivalent recognised system).

It is the responsibility of the lead recipient of all emails from third parties to ensure that they are captured in iShare (or equivalent recognised system). This is to preserve context and to maintain a comprehensive audit trail.

Ensure that sensitive information is only included in encrypted emails or those sent to a secure email address[6].

The Cabinet Office has issued guidance to government on dealing with Private Email Use which includes guidance relating to the Freedom of Information Act.

13 How do we manage records created by Private Offices and the Office of the Permanent Secretary?

Private Offices produce important records that need to be managed in accordance with the Public Records Act. Private Offices are comprised of the offices of ministers, the Permanent Secretary and other senior public servants, for example Director Generals, the Chief Medical Officer, the Chief Nursing Officer, the Chief Scientific Adviser, Agency Chief Executives and Regional Directors.

The records of Special Advisers (SpAds) require separate consideration. Where Special Advisers have a wider role within the Welsh Government and have an impact on official business, their records should be retained. If their records only mirror those existing elsewhere in the Welsh Government there is no reason for them to be kept as part of the official record. All papers that are concerned with party or parliamentary business should be kept separately and managed by the Special Adviser.

[6] https://documents.hf.wales.gov.uk/id:A6836735/document/versions/published

Private Offices must adhere to the information and records management policies and practices adopted by the Welsh Government.

Additional guidance is available here and also in the Archiving Policy for Generic Mailboxes in Private Offices

14 How do we manage EU Funded Records?

All relevant information and supporting documents relating to the work of the Welsh European Funding Office (WEFO) must be retained. This applies to both financial and non-financial information, to demonstrate compliance with EU rules and conditions.

These records must be retained until WEFO confirms that they are no longer required. Unlike previous programming periods, retention periods for beneficiaries are no longer linked to the Programme closure process, meaning that average retention periods will reduce to between 5 and 10 years from the date that expenditure has been declared to WEFO or, if applicable, to an Intermediate Body. In most cases, the retention period will be around 3 years following the end of the operation. See WEFO Guidance for further information.

15 How do we lawfully process and protect Sensitive Personal Information?

A strong data protection culture is closely linked to Information and Records Management, and Information Security.

The data protection principles[7] outlined in the GDPR and the Data Protection Act 2018 set out our main responsibilities. Sensitive personal data is information about an

[7] Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner

that is incompatible with those purposes; further processing for archiving purposes in the public

interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and individual's race, ethnicity, criminal offences committed (or the fact they have been subject to criminal proceedings), political opinions, religious beliefs and/or membership of a trade union. Sensitive personal data is afforded a higher level of protection than other information.

If you are working with personal data you will need to undertake a Data Protection Impact Assessment (DPIA) and Privacy Impact Assessment (PIA). You will require a Privacy Notice, and must be able to demonstrate compliance with the data protection principles.

The citizen has the right to get a copy of the information that we hold about them under Data Protection legislation. This is known as a subject access request. Before responding to a request for information held about a child, you should consider whether the child is mature enough to understand their rights. Information about children may be released to a person with parental responsibility. However, the best interests of the child will always be considered. It is important to remember that not all personal information is covered and there are 'exemptions' within the Act which may allow the Welsh Government to refuse to comply with a subject access request in certain circumstances.

The Welsh Government uses CCTV across its estate. This is carried out in accordance with the CCTV Code of Practice (ICO). The Welsh Government does not keep CCTV information for longer than strictly necessary to meet its purposes for recording it. However, where a law enforcement body is investigating a crime and asks for it to be preserved, the Welsh Government will give them opportunity to view the information as part of an active investigation.

16 How do we manage Data Sharing?

Welsh Government staff must agree data sharing protocols with external organisations prior to data exchange. If data sharing contains personal data, a link to the relevant policy must be provided so that staff are aware of the process and the need to gain approval before sharing. These protocols must specify:

- Who the sharing organisations are
- Legal status of the partnership
- Information to be shared
- Management process for the information and what will happen to it once objectives have been met
- Principles for storage and access to Welsh Government information

It is a principle of data protection legislation that the amount and level of shared personal data must be no more than what is needed for processing. This applies

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

equally to other non-personal data. The agreed retention and disposal schedule must state whether it will be returned to the originator, archived, depersonalised or destroyed.

17 How do we send data outside the European Economic Area (EEA)?

Protectively marked data is not normally acceptable for storage outside UK, but personal data must remain within the EEA. If you need to send data outside the EEA you must obtain agreement and permission from the Data Protection Officer (DPO). The requirement for personal data to be hosted in the EEA is detailed in the Project Managers' Security Handbook.

18 How do we manage records created in the course of collaborative working or through out-sourcing?

Welsh Government staff must ensure that information shared with other bodies, or held on our behalf by other bodies, is managed in accordance with this policy.

Contracts with third parties must include reference to information management procedures and responsibilities. The contract should stipulate how records created in the course of collaborative working or through out-sourcing will be managed, shared and protected. Responsibilities must be agreed and the protocol signed by each partner. The protocol must outline who will be responsible for:

- Access to Information requests (and who has responsibility for keeping those records)
- Information Security, Information Management and Data quality
- Retention and Disposal (requirement for records to be returned to the Welsh Government for medium to long term retention and/or disposal)

Assurances from third party suppliers must be obtained regarding the way they handle information. A minimum requirement is that Cyber Essentials has been attained by the company where personal or OFFICIAL-SENSTIVE information is processed. Specific requirements will be included in the accompanying Security Aspects Letter.

19 How do we manage Open Data?

We have developed an Open Data Plan for the Welsh Government. The Public Service sector in Wales generates and publishes a vast amount of data which, if opened up and shared, could provide numerous opportunities and benefits. Amongst these are the potential benefits to the UK economy which are highlighted within Digital First and the Welsh Government Digital Action Plan.

We use the UK Government Licensing Framework (UKGLF) and Open Government Licence (OGL)[8] to licensing the use and re-use of Welsh Government public sector information. The OGL does not cover the use of personal data. Re-use of personal data must comply with the Data Protection legislation.

20 How do we manage Changes in Machinery of Government / Transfer of Functions?

In the event of Machinery of Government changes and/or a Transfer of Functions, the Departmental Records Officer must be informed at the earliest opportunity by the project lead to ensure the transfer of vital business records takes place without the loss of information or interruption to business continuity. The Departmental Records Officer must be involved throughout the process to ensure that correct information and records procedures are followed and legislation met.

All decisions on the legal status[9], movement, disposal and destruction of information must be documented. When records are transferred, they must be accompanied by whatever has been used to identify and retrieve them - such as indexes (original or copy as applicable) or copies of relevant databases used to describe and track digital records.

Arrangements must be made via our ICT provider to ensure the handover of computer systems and/or storage media used to create and manage current and inactive digital records of the transferred business.

Full lists of files to be transferred (regardless of format), plus details of any outstanding FoI requests or sensitivity issues, must be documented in the official Transfer Agreement (to be drawn up by the Departmental Records Officer in collaboration with the transferring department). This Agreement must then be signed by both the transferring and receiving organisation. The transfer of information and records must be included in any legal steps required to implement the change in Machinery of Government process.

21 How do we manage Public Inquiries, Reviews and Tribunal records?

Public Inquiries investigate issues of serious public concern and establish the facts of past decisions and events. It is important that Public Inquiries are accountable for how they receive evidence, gather information, deliberate and report their findings.

A Public Inquiry must maintain an adequate record to:

[8] The Open Government Licence (OGL) is a simple set of terms and conditions that facilitates the re-use of a wide range of public sector information free of charge. The OGL is also available in Welsh.

[9] Transfer of information must be done formally as it is a transfer of information between two separate legal entities. This is not as straight forward as simply copying data.

- Demonstrate the conduct of the Inquiry and provide accountability for its findings
- Ensure that the Inquiry Panel and associated staff can access and retrieve information when required
- Secure records of historical/research value

Inquiry papers must be dealt with immediately after the Inquiry is completed. It is not necessary to wait until the papers reach the normal age for review. The secretary to the Inquiry must inform the Departmental Records Officer when the Inquiry is drawing to a close. Arrangements can then be made for the proper retention and disposal of records. Retained records will be transferred to TNA.

Search terms and search strategies employed to identify and retrieve information for an Inquiry will be agreed with the relevant Policy department. These terms and strategies will be documented and held on iShare as evidence of the searches that have been carried out on behalf of the Inquiry.

21.1 Inquiries or Tribunals independent of the Welsh Government

These records are the responsibility of the Inquiry and not the Welsh Government. The Inquiry/Tribunal Chair and Secretary must ensure that the Inquiry record is comprehensive and well-ordered and that the relevant policies and procedures are in place.

21.2 UK-wide and Welsh Government inquiries and/or reviews into child or other abuse

The Welsh Government needs to demonstrate that it has robust procedures which can withstand scrutiny and provide assurance that all allegations are referred to the appropriate authority and a secure record is kept.

If an allegation of abuse (e.g. child abuse or abuse at a care home) is made it must be recorded with the file (hard copy and/or digital) being marked up as significant. This marking will inform the Welsh Government (and if relevant, the Home Office) as to how to handle that file, its retention and the need to document when it is destroyed or deleted.

For wider abuse allegations, appropriate retention periods must be applied which can be justified in terms of the GDPR and Data Protection Act 2018.

A protocol agreement with the police must also be put in place on referrals and information sharing. This includes a system of recording what information is sent to the police and a formal procedure of confirming what the result of that reference is.

22 How do we manage Litigation / Legal / Document Hold, Hold Order and Preservation Orders

Information (or documents) may be required as evidence for legal purposes in several contexts. They may be required to obtain legal advice on behalf of the Welsh Government, for the purposes of “discovery” to other parties involved in litigation in which the Welsh Government is a party, or for production in court by an agency whether or not the Welsh Government is a party to the proceeding.

If you or your division are involved in an Inquiry, legal proceedings or any litigation, you must contact the Director of Governance, the Data Protection Officer, the Chief Digital Officer and the Departmental Records Officer (DRO) as soon as possible. They will issue an instruction directing employees to preserve, and refrain from destroying or modifying, records and information (both paper and digital, including email, mobile phone messages and social media) that may be relevant to the subject matter of a pending or anticipated lawsuit or investigation. A litigation hold helps to ensure that the Welsh Government complies with its duty to preserve information, including electronically stored information (ESI), in litigation or in connection with an investigation.

Organisations must preserve relevant information when it reasonably anticipates a lawsuit or investigation. Their duty to preserve stems from:

- A common law duty to prevent spoliation of evidence.
- Certain statutes and regulations, including the Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745).

A data Privacy Impact Assessment (PIA)[10] should be undertaken before releasing information to ensure that sensitive personal information not relevant to the legal proceedings is redacted in compliance with GDPR/DPA.

23 How do we manage Legal Discovery and Candour?

23.1 Legal Discovery

The Welsh Government has an eDiscovery tool to help us with our “information explosion” and to cope with making this information available for public inquiries, court cases and internal investigations. It is also used to sift through our information to identify what needs to be kept and what needs to be deleted, and to ensure compliance with data protection legislation.

23.2 Candour

As a public authority, the Welsh Government has a “duty of candour”. This requires that we give a "true and comprehensive" account of the Welsh Government’s decision-making processes. It requires us to set out, fully and fairly, all matters that are needed for the fair determination of a particular issue. The duty extends to information or documents which will assist a claimant’s case, and those which give rise to additional grounds of challenge.

The duty of candour can be satisfied by giving a full and fair account in a witness statement, and exhibiting key documents. However, where a judicial review includes

[10] In providing essentially a trail of data deletions and transfer, a PIA can be immensely useful for the purposes of discovery, both in demonstrating compliant data transfer and retention, but also by providing defensible deletion records in the context of disclosure requirements and obligations. The PIA can also demonstrate how PII in a data set was reduced, eliminated or remediated.

issues of fact, or requires the court to consider proportionality, more documents may need to be disclosed.

Under the duty of disclosure, “a document” includes deleted documents, so even if deleted documents are no longer retrievable, the fact they existed must be disclosed. The duty of disclosure requires a reasonable search, and requires a party to state if they have decided not to search for a category or class of documents on the grounds that it is unreasonable.

24 How do we manage Retention and Disposal?

Information and records will only be retained for as long as they are needed to support the Welsh Government’s business requirements and legal obligations. At the end of that time, the records will either be destroyed or, if they are historically valuable, transferred to a Place of Deposit for permanent preservation.

The Welsh Government’s Retention and Disposal Schedule is the key to effective information management: it sets out the recommended periods for which particular classes of information must be retained in accordance with legal, audit and operational requirements. It provides a formalised, accountable system for the retention and disposal of information and can help to save time, money and space by ensuring that it is not kept unnecessarily.

The GDPR and the Data Protection Act 2018 set up additional requirements around retention of personal data. After the expiration of the applicable retention period, personal data does not necessarily have to be completely erased. It is sufficient to anonymise the data. This may, for example, be achieved by means of:

- regularly deleting information no longer required – e.g. staff information, CV’s, application forms
- erasing unique identifiers which allow the allocation of a data set to a unique person
- erasing single pieces of information which identify the data subject (whether alone or in combination with other pieces of information)
- separating personal data from non-identifying information (e.g. an order number from the customer’s name and address)
- aggregating personal data in a way that no allocation to any individual is possible
- storing personal data in an appropriate area with the correct authorisation access controls, and retention periods
- listing sensitive personal data on the Information Asset Register (IAR)
- complete Privacy Impact Assessments (PIAs) where appropriate

25 How do we select records for transfer to TNA or other Place of Deposit?

In line with the Public Records Act 1958 and the Freedom of Information Act 2000 (Section 46), the Welsh Government was required to dispose of or transfer all records to a Place of Deposit by the time they reached thirty years old (known as the 30 Year Rule) so that they could be made available to the public.

As a result of the Constitutional Reform and Governance Act (CRAGA) 2010, a reduction from 30 to 20 years was introduced in January 2013. This will be a gradual reduction over a ten year period. We will transfer two years' worth of records where we would normally only transfer one (i.e. in 2013 we transferred records from 1983 and 1984, in 2014 we transferred records from 1985 and 1986 etc.). The reduction will therefore be completed by 2023 when records created in 2003 will be ready for transfer, and the 20 Year Rule will become "business as usual". To monitor progress, the National Archives will collate and publish our transfer objectives / achievements once a year in the Information Management Report.

The Government of Wales Act 2006 (Part 6, sections 146-148) makes provision for Welsh public records, carrying forward provisions originally made in the Government of Wales Act 1998. The 2006 Act means that, if requested, the UK Department of Media, Culture and Sport (DCMS) can create an Order under section 147 to make Welsh Ministers or a member of the Welsh Government responsible for preserving our records. As part of this Order, all the necessary arrangements to store, preserve and provide access to public records must be made and the National Archives (TNA) informed accordingly.

However, Wales does not currently have its own national archive comparable to the National Archives, the National Archives of Scotland or the Public Record Office of Northern Ireland[11]. The cost implications of establishing such an archive for Wales are prohibitive and so the National Archives remains the recognised repository for Wales as well as the UK government, and a memorandum of understanding exists to

[11] Arrangements in other devolved regions in the UK

NORTHERN IRELAND

Northern Ireland: Legal basis:

Public Records Act (Northern Ireland) 1923

Archival responsibilities:

The Public Record Office of Northern Ireland (PRONI) is the only public archive service in Northern Ireland. It is thus responsible for the archives of every aspect of government activity in Northern Ireland, including those of the work of UK government departments relating wholly or mainly to Northern Ireland.

SCOTLAND

From 1 April 2011, the General Register Office for Scotland merged with the NAS to become the National Records of Scotland (NRS).

Scotland: Legal basis:

Public Records (Scotland) Act 2011. This act replaces the Public Records (Scotland) Act 1937.

Archival responsibilities:

The Keeper of the records of Scotland as head of the National Records of Scotland is responsible for the archives of all national agencies, except those of the Registrar General (Civil Status), but including those of parliament and the law courts, and those relating wholly or mainly to Scotland transmitted from government departments with UK responsibilities. The Keeper's approval is required for the archival management systems put in place by local authorities.

formalise this relationship. The Chief Executive of the National Archives, on behalf of DCMS, is required to supervise the current arrangements for Welsh public records until such a time as an Order under section 147 is made.

A review is conducted of all records as they reach the end of their retention period and the relevant departments are consulted in order to decide which records are of no further use and can be destroyed; which records need to be retained by the department for on-going business use; and which records have historical value and should be transferred to the National Archives.

The selection of records with historical value is conducted in accordance with the National Archives' Records Collection Policy and our own Operational Selection Policies. We liaise with a dedicated Information Management Consultant at the National Archives to review and validate our appraisal decisions. Once agreement has been reached, we prepare the records for transfer (cataloguing, "cleansing", sensitivity reviewing) before they are accepted by the National Archives. We have a Sensitivity Review Policy which outlines how such a review should be undertaken.

For records needing to be retained by departments beyond this period (e.g. where they have a long-term business need, or where the information is subject to an on-going inquiry) we must apply for permission from the Advisory Council (for a "Retention Instrument") to avoid being in breach of the Public Records Act.

26 How do we preserve our Information?

Access to digital information for both short and long term business requirements is vital. A Digital Continuity project was conducted in 2010 to assess the requirements of digital preservation and to explore appropriate solutions to ensure continued access to, and the integrity of, digital information.

To ensure that digital information remains accessible and future-proof, provision has been made as part of the information management process to migrate digital material held on iShare to the most recent versions of software on a regular basis. This means that current information will always be accessible during its lifetime, but it also means that information which has been identified as having historical value will continue to be accessible for future generations.

27 How do we manage Copyright - Intellectual Property of Others?

A document must not incorporate the intellectual property of others unless the Welsh Government has the relevant rights i.e. Crown copyright. Staff will not enter documentation (including scanning) into an information system (e.g. iShare, shared drives, PPIMS, etc.) unless the Welsh Government owns or has obtained the copyright to do so. Material specifically addressed to the Welsh Government can be entered into an information management system.

See Adding Copyright Documents to iShare for further guidance.

Some social media sites, such as Facebook and Twitter, currently state in their Terms of Usage that content remains the intellectual property of the individual or entity that posts the content. This is not, however, the case for all social media sites, such as YouTube, who assert copyright over content posted on their platform.

Information kept in an Electronic Document and Records Management System (EDRMS), a shared drive or other bespoke system (such as SharePoint) can be simultaneously accessed by multiple users. This constitutes 'replication' or in some cases a 'broadcast' under copyright legislation, leading to the possibility of an individual claiming compensation for copyright infringement for content published to a social media site being stored in an EDRMS or other system by a government organisation.

28 How can the public gain access to Welsh Government Public Records?

28.1 By searching the National Archives' Catalogue

Most historical Welsh Government information over thirty years old (currently being reduced to twenty years - see paragraph 23) is held at the National Archives and is available for the public to view. It is possible to search the National Archives' online catalogue by keyword, date range, places, people, and the relevant file series code (which is "BD" for Welsh Office records and "WA" for Welsh Government records).

Current Welsh Government information can also be viewed online on our external website.

28.2 By placing a Freedom of Information Request

Requests for information less than thirty years old must be handled in accordance with the Freedom of Information Act 2000. Advice on requesting information can be found under Access to information - How to ask for information on the Welsh Government external website.

28.3 By placing a Data Subject Access Request

Please follow the guidance for placing a FoI request above.

29 How do we ensure the re-use of Welsh Government Publications?

29.1 Publications catalogue

To comply with the Welsh Government's Publication Scheme (a requirement under the Freedom of Information Act) and the Re-use of Public Sector Information Regulations 2005 (S.I. 2005/1515), and subsequent amendments known as 'the PSI Regulations') we need to make sure that our research reports and publications are available to the public.

Our organisation undertakes and commissions research relevant to its responsibilities and produces regular reports which are often published on our corporate website. To ensure that these are available and accessible over time, the Information & Archive Services team catalogue them so that members of the public can access or request them via the external online Publications Catalogue.

Colleagues should email all electronic Crown Copyright published material to Library-Enquiries so that they can be catalogued within one month of the date of publication.

29.2 Legal Deposit

To comply with the UK's legal deposit legislation, a copy of every Welsh Government print and digital publication[12]must be given to the British Library and the National Library of Wales.

30 What Information and Records training is available?

We have a mandatory training course on our corporate training portal for all Welsh Government staff. This e-learning module provides staff with an introduction to the key concepts of good information management. It will enable staff to identify:

- who is responsible for information management
- what a record is
- recordkeeping responsibilities
- where to go for help

Further advice and "How Do I …?" guides are available on our intranet pages under iShare Guides.

All staff must undertake the mandatory e-learning course, "Responsible for Information" every two years. Those in Inspectorate and Advisory areas must complete it on an annual basis.

31 How do we monitor and report on Information and Records Management?

We work with The National Archives who monitor compliance on a regular basis through Information Management Assessments.

Information and Records Management compliance is reported in the Welsh Government's Internal Control Questionnaire.

32 What do we do with our information when leaving the Welsh Government?

People leaving the Welsh Government's employment are responsible for ensuring that they deal with any information and records they have been working on before departure to ensure that:

- Work can be carried on by a successor, without delay
- Welsh Government can be accountable for their work after they have left

[12] Materials covered by legal deposit include printed books, journals, magazines and newspapers, microfilm, publications on hand-held media such as CD-ROMs, websites and material available via download.

- Welsh Government complies with the GDPR, Data Protection Act 2018 and Law Enforcement Directive (LED)
- Welsh Government can respond to Freedom of Information and Subject Access Requests accurately and within the legal response times
- Welsh Government does not incur unnecessary expenditure on records storage and staff time sorting out others' records

No Welsh Government information should be retained by the leaver. See the How Do I… guide.

Annex A

Paragraph 6 of the WPC User Guide:

6. Retention of WPC Transaction Records

6.1 On receipt of your WPC the Card Administrator will issue you (the cardholder) with an iShare file solely for the purpose of the electronic retention of your WPC receipts, invoices, statements and authorisations.

6.2 You must ask for a receipt where one is not automatically offered. You must retain the full itemised receipt, credit card stubs are not sufficient. You are advised to check a receipt when it is given to you as dates and times are not always accurate. You must scan or photograph any receipts and upload them into your iShare file, giving them a title that corresponds with the description in BSM as outlined in paragraph 6.4. If any details on the receipt are not clear or if you find an error, you must produce an explanatory note and upload this to iShare too. You must not amend or annotate the receipt in any way. It is not necessary to place the physical receipt (including those relating to European funded programmes) on a registered file once it has been scanned or photographed and placed into iShare.

6.3 You must ensure that all scanned or photographed records saved in your iShare file are eligible. All records must be retained for a period of at least 7 years after the end of financial year in which the payment was made and 12 years from the date of the closure of the relevant programme if the payment was made from an EU funded programme. These records must be produced for inspection if requested by any authorised person. This may be an internal inspection team, a Welsh Government or Wales Audit Office auditor or any other authorised official such as a line manager. Copies of receipts can also be demanded by Her Majesty's Revenue & Customs (HMRC) who have statutory powers of inspection.

6.4 Each invoice/receipt must be given a unique reference number and this must be entered in the description when the document is saved in I-Share. This unique reference must then be entered in the transaction description on BSM along with a description of what has been purchased.

6.5 In exceptional circumstances where receipts are not available a clear explanation should be provided in a file note countersigned by the transaction approver and upload this into your iShare file. You must follow the guidance in paragraph 6.4 for retaining and logging these documents on BSM.

6.6 Cardholders who do not have access to iShare should where possible make arrangements for a colleague within their directorate to upload the receipts for them. If this is not possible the Card Administrator will in exceptional circumstances arrange for a physical file to be issued.