Policies and Procedures

Privacy Notice for JNCC staff and former staff

Privacy Notice for JNCC staff and former staff

Purpose

JNCC collects and processes personal data relating to its employees for various reasons and this privacy notice sets out what data is collected and processed and the lawful bases for processing the data. The organisation is committed to being transparent about how it collects and uses personal data and to meeting its data protection obligations.

How we use your information

For the employment contract
JNCC needs to process data to enter into an employment contract with you and to meet its obligations under this contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer your benefit and pension entitlements. This data includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- information about your marital status, next of kin, dependants and emergency contacts;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration and entitlement to benefits such as pensions;
- details of your bank account and national insurance number and any travel and subsistence claims you make;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including probationary reports, performance reviews and ratings, performance improvement plans and related correspondence; and
- references supplied by former employers (collected from third parties).

For compliance with JNCC's legal obligations
In some cases, JNCC needs to process data to ensure that it is complying with its legal obligations. This data includes:

- information about your nationality and entitlement to work in the UK, to comply with the Immigration, Asylum and Nationality Act 2006;
- information about your criminal record, to comply with the Government baseline personnel security standard;
- details of your attendance at work and periods of leave taken by you, including sickness absence, special leave, and the reasons for the leave to ensure that you are receiving the pay or other benefits to which you are entitled, to comply with the Employment Rights Act 1996 and the Working Time Regulations 1998;
- some special categories of personal data about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments and which is processed to comply with the Equality Act 2010 and Health and Safety at Work etc Act 1974; and
- staff salary information within statutory reports (remuneration report in the ARA) and statutory accounts;

Supporting our public task or legitimate interests
In other cases, JNCC needs to process data in pursuit of our public task or other legitimate interests before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- collect time recording information individually in order to track time spent on Grant in Aid and income projects to ensure an accurate representation of staff resource against project codes. This supports our contractual obligations for income projects and duty to the Treasury to account for and spend public money efficiently.
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of employee skills, to identify skills gaps, to enable effective resource and project planning, continuing professional development and identifying key skills and capabilities for income generation purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management;
- ensure effective general HR and business administration; provide references on request for current or former employees;
- Protect safety of staff, the building and our assets (by using your image for a security pass and CCTV to manage entry into JNCC offices);
- respond to and defend against legal claims;
- record and review any complaints against staff/JNCC and administer Subject Access Requests. Also administer staff questions for open meetings and share stories through the weekly staff update;
- run projects, create outputs, maintain audit trails; including cataloguing datasets;
- bid for potential income generation opportunities and record time against projects to recoup costs; for which data will include:

    - your personal data in CV format. You will be reminded to update your CV on an annual basis to keep it up to date;
    - should the income opportunities be successful, your personal data in the form of time recording/payroll information and electronic signature may be required to allow JNCC to recover income for any time spent on the project. It might be necessary to re-format or re-word CVs in line with bid requirements and in consultation with the data subject;
    - educational certificates if requested for bids will be collected on a case by case basis. They will only be stored in restricted access bid folders (not centrally); and
    - time recording data against projects.

- model expenditure on salaries and expenses for monitoring and forecasting and forward planning;
- provide our staff with corporate credit cards as needed;
- for the prevention and detection of fraud;
- enable staff across teams and offices to identify each-other through the staff profiles section of the intranet; and
- raise the profile of JNCC and its staff by:

    - publishing biographies (including images) through its website
    - publicising staff attendance at events or other activities through social media; and
    - publishing details of staff who contributed to a scientific paper, report or other publication.

Equal opportunities monitoring
You are under no obligation to provide this information and there are no consequences or detriment to you if you choose not to provide it or later remove it by choosing "prefer not to say". We process this data with your explicit consent because you are not obliged to give it, you can withdraw it at any time by logging in and removing the data. If you choose to supply your special category data via OpenHR Self-Service, it will be used for equal opportunities monitoring and it will also be processed:

- to identify or keep under review the existence or absence of equality of opportunity or treatment between groups of people specified in the Data Protection Act 2018;
- to perform or exercise our obligations or rights as the controller, or your obligations or rights as the data subject, under employment law, social security law or the law relating to social protection; and
- to ensure we meet our requirements of the Civil Service Commission Recruitment Principles.

Staff Equality Diversity and Inclusion Reporting Portal
The JNCC EDI group has set up a form to provide a space for staff to share EDI related ideas, concerns or to report any EDI related incidents of bullying/misconduct. The form is automatically anonymous, but a respondent can supply name and email if they require a response from the EDI group. The information supplied will be used to understand the specific needs of JNCC employees with regards to EDI, help to gauge the progress of the EDI group's actions and highlight problems within the organisation.

JNCC's EDI group is collecting name and contact email, only if supplied, to be able to report back on the progress of the response supplied via the form. We are doing so with consent, and in the case of providing special category data, explicit consent.

Portal responses will be stored securely in Office 365 as part of the forms cache and as an auditable database in the closed EDI Group TEAMS channel. Any responses with personal information will be stored for up to 6 months after the resolution or acknowledgement of the response, from which it will be anonymised and form part of the auditable database.

Responses relating to incidents of bullying, harassment or misconduct that the respondent has asked to be forwarded to HR will be subject to a separate retention policy. Respondents should not name other people in reports, any reports of bully, harassment or misconduct naming someone should go through the official channels outside of this process.

Storage and protection of employee personal data

Data will be stored in a range of different places, including in your personnel file, in the organisation's HR database (OpenHR), in restricted network drives (Y: Drive, Z: Drive) and in other IT systems (including the organisation's email system). Further information can be found in the Electronic File Storage Policy.

JNCC takes the security of your data seriously. The organisation has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Sharing of employee personal data

JNCC shares your data with third parties that process data on its behalf in connection with payroll (SSCL), the provision of benefits, pensions (MyCSP) and the provision of occupational health services (Duradiamond). Where JNCC engages third parties to process personal data on its behalf, we do so on the basis of written instructions, are under a duty of confidentiality and will implement appropriate technical and organisational measures to ensure the security of data.

JNCC may share your data, if sharing is part of a legal obligation; for example, employment information we need to provide to Office of National Statistics. We also need to provide a monthly financial report to DEFRA which includes names and addresses.

When an employee goes on a secondment, JNCC will share personal data with the host organisation for the effective performance of the secondment agreement and for legitimate managerial and administrative interests.

Your CV and, if requested for bids, your educational certificates, will be shared with potential business partners and funders where JNCC is bidding for work and may need to be shared with other JNCC colleagues if they are the lead on the bid. You will be reminded to update your CV on an annual basis to keep it up to date. You will be informed when it is being shared and consulted with if amendments are required. We will ensure such parties are demonstrating adherence to UK data protection standards. Should we be successful in securing further income projects we may need to provide time recording and payroll information to the funding agency. We may also require an electronic signature to be used for the claim.

Directors have access to CVs to increase their knowledge of staff capabilities, assist in skills gap identification, and to better help promote JNCC.

JNCC will also share your data where arranging travel or accommodation for you, or for other purposes as needed in line with this privacy notice.

Whenever we transfer personal information to countries outside of the European Economic Area in the course of sharing information as set out above, we will ensure that the information is transferred in accordance with this Privacy Notice and as permitted by the applicable laws on data protection.

Length of data retention

JNCC will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out within the Retention and Disposal Protocol .

Your data that has been used for specific bids or income generation projects may need to remain on file for a further 10 years following completion of the project. Should the bid be unsuccessful, we will remove any personal data from the bid folder one year after receiving notification from the funder.

Your rights

You can access and obtain a copy of your data on request by contacting us with the details of what you would like to be provided. You can also ask us to change incorrect or incomplete data, delete or stop processing your data. Where we have previously relied on consent for us to use your data you can withdraw at any time.

If you have any questions or concerns about how your data is being used, or to progress any of your rights mentioned above, please contact our Data Protection Manager:

Email: dataprotection@jncc.gov.uk

Address: Joint Nature Conservation Committee, Monkstone House, City Road, Peterborough, Cambridgeshire, PE1 1JY

The Data Protection Officer responsible for monitoring that JNCC is meeting the requirements of Data Protection legislation is based within Defra and can contacted via:

Email: DefraGroupDataProtectionOfficer@defra.gsi.gov.uk

Address: Defra Group Data Protection Officer, Department for Environment, Food and Rural Affairs, SW Quarter, 2nd floor, Seacole Block, 2 Marsham Street, London SW1P 4DF

If you have any concerns about how your data is being used, we will endeavour to answer any questions you have. You have the right to lodge a complaint with the Information Commissioner's Office. You also have the right to an effective judicial remedy against decisions of the Information Commissioner's Office, or against JNCC.

Changes to this privacy notice

We keep our privacy notice under regular review. This privacy notice was last updated on **8 April 2021**.

03/07/2018 - Added "staff salary information within statutory reports (remuneration report in the ARA) and statutory accounts" under Legal Obligations.

14/08/2018 – Added details of data shared during staff secondments.

03/09/2018 – Added for the detection and prevention of fraud to employee details uses

05/08/2019 - Added "Directors have access to CVs to increase their knowledge of staff capabilities, assist in skills gap identification, and to better help promote JNCC."

07/02/2020 – Added explicit consent legal basis to Equalities Monitoring data information.

8/10/2020- Added time recording processing under public task

03/03/2021- EDI reporting portal added

08/04/2021- rewording of the Equalities Monitoring data information to improve clarity (no change to the way it is processed)

Policies and Procedures

Retention and Disposal Protocol

Last reviewed: March 2019

Contents

JNCC Retention and Disposal Protocol

1. Purpose and Coverage

1.1. This protocol sets out how staff are expected to review, retain and dispose of information held by JNCC.

1.2. Some information comprises evidence of decisions, actions and activities for business, legal or regulatory purposes, or has a higher ongoing value to the organisation. Rules for protection and management of this information are more stringent.

1.3. Effective file management will simplify the task of finding information to meet corporate, day-to-day, and legal requirements, reduce duplication and confusion, and reduce maintenance costs and the risk of security breaches.

2. Introduction

2.1. JNCC has a corporate responsibility to manage 'records' created or received in the course of normal business, in accordance with regulatory requirements and best practice. Records are defined by the National Archives as "Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business". Records are an important resource for the operation of an organisation, and are essential to protect and preserve the evidence behind key decisions.

2.2. Good records management is vital for business continuity and transparency. Standards for retention and disposal of some records are also determined by legislative requirements. For example JNCC may need to retain records to defend against legal claims until the relevant time limits in the Limitation Act 1980 expire, or may be required to be disclose information to the public under the Freedom of Information Act (FOI) or Environmental Information Regulations (EIR), or need to ensure that records containing personal data are anonymised or disposed of in compliance with data protection legislation. Please see Annex C for a summary of the main legislation.

2.3. Staff responsibilities for managing JNCC's information are outlined in the JNCC Information Management Policy. All staff have a responsibility to comply with this policy, exercise good judgement and due diligence, and manage the information which they create and handle in an appropriate way, in line with JNCC's information management framework. Staff should raise any queries and concerns about records management with the relevant Information Asset Owner (IAO) and direct further

queries to JNCC's Information Management and Data Protection Manager or Departmental Security Officer.

3. Reviewing information

3.1. JNCC periodically holds an organisation-wide 'greening day' for staff to review their active and historical files in line with JNCC's retention schedules (Annex A). However records management is an ongoing activity. This activity is essential to ensure that JNCC can find information on an ongoing basis, and also reduces the potential for file duplication, stagnation and loss of information.

3.2. Staff should work with their IAO to plan their approach to the review process. In general document types with a higher level of risk, such as records that contain confidential information or sensitive personal data, should be given priority. With respect to records containing personal data, the objective is to ensure that all personal data held in each work area is within its retention period and that any personal data that is near (or beyond) the end of its retention period is either reviewed for further retention or scheduled for deletion. Please see section 4 on Retaining information and section 5 on Disposing of information.

3.3. Staff should work through the retention schedule in Annex A, identify which document types they hold within their work area, and identify which of that information is due for review. The target information should then be reviewed and either labelled as 'retained' or scheduled for deletion. Staff should take a risk-based approach, prioritising certain document types or collections of records including project files.

3.4. Additional 'greening' activities should be undertaken throughout the year as necessary – for example during staff handover, at the end of a project, or when the risk around a particular collection of records increases beyond JNCC's risk appetite.

3.5. The retention schedules in Annex A will vary according to the particular material and scenarios. The significance of a file or collection of information could increase during its life i.e. a record may become of historical interest because of changes in government policy or legislation.

3.6. Records should not be disposed of automatically when they reach their scheduled end of retention. Staff should review the retention period before disposal to determine whether there is any basis for extending the period.

4. Retaining information

4.1. Once reviewed, a decision must be taken to retain or dispose of the information.

4.2. Information should be retained if necessary to meet legal requirements such as those in the Limitation Act 1980 or the General Data Protection Regulation (GDPR), or if the information:

- provides evidence of decisions or actions taken by JNCC that is not documented elsewhere,
- is necessary for operational use or to protect corporate knowledge – 'corporate knowledge' in this context means who in JNCC should act, what should be done, when should it happen, where work should be conducted, why it is important, and how to do it, so that JNCC can operate effectively,
- is relevant for historical research or has cultural value,
- covers issues of national interest, or
- contains information that is likely to be reused at a later time as either reference material or to support subsequent work.

4.3. If there is an identified need to retain a record beyond its established retention period, but a need for permanent retention has not been identified, staff should annotate the record as having been reviewed and set a date for the next review. Most electronic records can be annotated using the properties within the document. For example to access the property fields in Microsoft Word and Excel documents, select the File tab, then Info and Properties. Use the Comments field to specify that the record has been reviewed and will be retained.

4.4. Some information created or held by JNCC should be retained permanently. This include records that meet any of the following criteria:

- records relating to the establishment of JNCC (organisation, staffing functions, operations),
- principal policy papers, e.g. submissions to ministers,
- records relating to formulation, implementation or interpretatin of policy, in particular thoe that reflect major changes in policy, principles and programmes,
- evidence of key decisions that have had a significant national impact,
- records that show interactions between JNCC and other public sector bodies, or show JNCC's participation in the scientific community, in particular those that contain statistics or returns not available elsewhere,
- records relating to preparation of support for or opposition to principal legislation on a national, European or tinternational level, and
- datasets and other digital materials to which a DOI has been allocated.

4.5. In some cases the retention period will be guided by a commitment to public access or re-use of information. There is a particular need to ensure the long-term retention of datasets and other digital materials that JNCC has made available for public access or re-use on terms where there is an expectation of preservation or ongoing availability. If JNCC has made a dataset available for public re-use under an open licence or under another type of perpetual licence, both an internal copy of the dataset and any records necessary to demonstrate the legal provenance of third-party intellectual property contained in the data should be retained indefinitely. Please refer to the Open Data Policy for background. Additionally, if JNCC has assigned a Digital Object Identifier (DOI) to a dataset or other digital material this means there is a firm intention to maintain permanent accessibility of the material outside JNCC, with a plan for the long-term preservation. Please see the DOI Protocol for background.

4.6. Following is a longer list of factors that may influence decisions on setting retention periods. Staff may wish to consider whether:

- the information is relevant to a significant decision or an organisational change,
- the information underpins a research output or advice JNCC has given,
- the information is relevant to the lineage or provenance of any output or process,
- the information might be required as evidence in a future audit process,
- the information is likely to be useful as a reference to inform JNCC's work or understanding of a scientific subject,
- JNCC holds the only copy of the information, or the authoritative copy,
- the information has been deposited with JNCC on the understanding that we will archive it,
- JNCC has published the information or made a public undertaking to maintain its accessibility,
- deletion of the information would harm the interests or rights of a data subject,
- retention or disposal of the information is required by law,
- the information is subject to a contractual requirement that requires its retention or deletion,
- the information is relevant to an ongoing legal process or is in scope of an ongoing information request,
- there are limitations on the availability of storage space, and
- the physical medium is viable (for example deteriorating paper, old film stock, floppy discs, and electronic file formats not supported by current software).

5. Disposal of information

5.1. Electronic records. Disposal of records occurs when the owner has reviewed a record either on an ad oc basis or according to the retention schedule, and made a decision to destroy it. There are several methods for disposal of records. Records in electronic formats are disposed of by deletion. Great care should be taken before deleting electronic records as they may not be recoverable.

5.2. Paper records. Paper records should be disposed of appropriately. Official and non-confidential paper records should be torn up or shredded and then disposed of for recycling. Staff should consider whether it is sufficient to tear up a document or whether a shredder should be used, based on the risk of targeted reconstitution of the information. Confidential or sensitive information, including documents designated as OFFICIAL-SENSITIVE, must be shredded using a cross-cut shredder, prior to recycling. Please contact the Admin Services Team for guidance on the locations of shredding machines. A secure disposal service also available for large quantities of paper records.

5.3. IAOs are responsible for deciding within their programmes which information and document types should be logged upon disposal. A template for this purpose is provided in Annex B. Disposal of records designated as OFFICIAL-SENSITIVE requires the specific authorisation of the relevant IAO. Disposal of records after review, prior to the end of a retention period established previously, also requires the specific authorisation of the relevant IAO.

5.4. The following information may be disposed of without specific authorisation:

- Duplicate records.
- Working drafts, where the results have been written into a final JNCC document and which are not necessary to support it. However any decisions that have been captured in working drafts (e.g. ignored comments) should be logged elsewhere – please see the JNCC Evidence Quality Policy for more information.
- Ephemera. These records and documents include notices of meetings and events, announcements, invitations, acceptances, internal admin requests such as resource reservations, travel bookings, etc.
- Personal entries and reference sources maintained by individual staff. This may include personal emails, photographs, and correspondence.
- Conference and training material. This material should be kept only while relevant or useful.
- Licensed material where the licence has expired. Datasets and other material licensed from third parties for a fixed period should be either deleted at the end of the licence period or returned to the licensor, unless the terms of the licence allow longer retention. The specific requirements will depend on the terms of the licence.

5.5. When disposing of IT equipment such as hard drives and printers, all digital information must be erased before the equipment leaves the office. Staff should seek advice from IT Support if unsure how to erase information securely.

6. Archiving and deposit services including web archiving

6.1. The National Archives is the UK Government's authority on records management and compliance with the Public Records Act, and includes requirements for transfer

of public records for archiving by National Archives. As JNCC is a non-departmental public body (NDPB), and has not been brought within PRA by any other legislation or order, JNCC's records are not within scope of PRA. This means that JNCC does not normally deposit records with National Archives for retention or preservation. However JNCC does make reference to National Archives guidance on records management as a source of good practice.

6.2. JNCC web domains are currently within the non-statutory scope of the UK Government Web Archive, a National Archives programme to capture, preserve, and make accessible UK central government information published on the web from 1996 to present. National Archives periodically makes copies of material on JNCC websites and republishes it as a snapshot for ongoing public access. This process is at the discretion of National Archives and JNCC should not rely on the UK Government Web Archive as a substitute for its own retention of records or as a basis for meeting any legal requirements for data retention.

6.3. Copies of any publications that JNCC produces with either an ISBN or ISSN are deposited with the British Library. Copies of these publications held by JNCC for purposes of its own work are subject to normal retention and review periods.

7. Personal data in records

7.1. Storage, erasure and destruction of personal data are all types of processing within scope of the General Data Protection Regulation (GDPR), the Data Protection Act 2018, and other data protection laws. Retention and disposal of JNCC records containing personal data must comply with these legal requirements.

7.2. 'Personal data' means any information relating to an identified or identifiable living natural person (the 'data subject'). Please see JNCC's Data Protection Policy and guidance for more information on personal data and data protection.

7.3. Data protection requirements apply to personal data in electronic records, and to personal data in paper records that are kept within a filing system. A 'filing system' for this purpose is any structure that makes the data accessible according to specific criteria, whether centralised, decentralised or dispersed, and includes for example paper records in a filing cabinet or on shelving that are labelled or sorted by name, date, function, or job title.

7.4. The 'storage limitation' principle in GDPR requires that personal data shall be "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". However, as ICO guidance says, GDPR does not dictate

how long a data controller should keep personal data. It is up to JNCC to justify retention periods for personal data based on the purposes for processing.

7.5. GDPR also requires that processing of personal data should be limited to that which is necessary to achieve lawful purposes, and that personal data should be protected with appropriate security. This means that access to personal data should be restricted based on its sensitivity and the purposes for which it will be used. While reviewing files for retention and disposal, JNCC staff should take note of any records that contain personal data and where necessary ensure that access to those records has been restricted to relevant staff.

7.6. As an organisation engaged in scientific work, JNCC will often have legal latitude to retain personal data for the following further purposes, provided that JNCC has established a lawful basis of its own to process the data for some previous purpose:

- archiving purposes in the public interest,
- scientific or historical research purposes, and
- statistical purposes.

7.7. There should normally be no need to redact personal data from any JNCC record if the record will be retained with appropriate access and safeguards in a location under JNCC's administrative control.

7.8. Data subjects have a right to be informed about how their data will be processed, typically through a privacy notice. Privacy notices must include information on the retention period or the criteria used to determine the retention period. JNCC must ensure that actual retention of personal data is consistent with the information provided to data subjects.

7.9. For purposes of setting and communicating retention periods for records that contain personal data, staff should bear in mind that electronic records may be stored in backup systems for up to one year after deletion from operational systems. Backup periods should be taken into account when calculating retention periods.

7.10. GDPR places restrictions on processing of personal data outside the European Economic Area. This is a consideration if JNCC uses contractors to archive or dispose of JNCC records, or stores personal data on servers located outside the EEA.

Annex A Retention Schedule

Every piece of information should have a lifecycle that is either Temporary, Short, Medium or Long. The following definitions are adapted from Defra guidance:

Temporary lifecycle: delete at or before 12 months.

Low value, short-lived information that has no business benefit beyond weeks or months, for example agendas, photos from away days, conference slideshows, training arangements, duplicates, invitations, etc.

Short lifecycle: delete at or before three years from the date it is saved (or last modified).

Limited lifespan information such as minor drafts, copies, routine FoI/EIR requests, senior briefings, complaints, local management issues, business continuity plans, and information that has been published in full in paper format or on the JNCC website.

Medium lifecycle: store for seven years from the date it is saved (or last modified) and then delete.

This includes most routine business correspondence, financial information, operational /casework files, some legal cases, and routine information produced by policy or advisory units (but not policy decisions or formal advice).

Note – for registered paper files with financial information, keep for 6 years after the last financial transaction of the file (not the date of first paper). In many cases this will mean retaining the paper file for 11 years (i.e. 5 years for the usual lifespan of the file + 6 years). Also note – some HR information within this category will be reviewed after 6 years.

Long lifecycle: has a business life of longer than seven years or is of potential historical or scientific value. Normally there should be no reason to delete or destroy this information unless there is a legal requirement to do so.

Includes evidence of principal funding decisions, key research, information from major JNCC-led committees or partnerships, submissions or significant advice to government, significant organisational changes affecting the way JNCC works, details of high profile events, significant legal advice, HR files, property files.

The following schedule is derived from disposal and retention schedules suggested by the National Archives and similar schedules in use by other public sector organisations. However these categories are generic and actual schedules may be varied based on the particulars and content of individual records.

Review at the end of the retention period unless another review period is indicated.

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
Corporate, Science, International and Marine Records	Advice to stakeholders	Long	Keep at least 25 years and then review every 5 years
	Strategies	Long	Keep at least 25 years and then review every 5 years
	Organisational history and records of significant organisational changes	Long	Keep at least 25 years and then review every 5 years
	Minutes and papers	Long	Keep at least 25 years and then review every 5 years
	Survey and monitoring data and reports	Long	Keep at least 25 years and then review every 5 years
	Guidance or technical reports for stakeholders	Long	Keep at least 25 years and then review every 5 years
	Research outputs	Long	Keep at least 25 years and then review every 5 years
	Written particulars of employment, contracts of employment incl. the Certificate of Qualification or its	Long	Keep until age 100 of data subject

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
Employee & Records	equiv. and incl. Senior Civil Service; changes to terms and conditions, incl. change of hours letters		
	Job history – consolidated record of whole career, location details – paper or electronic	Long	Keep until age 100 of data subject
	Current address details	Medium	Keep 6 years after employment has ended
	Record of location of overseas service	Long	Keep until age 100 of data subject
	Variation of hours – calculation formula for individual	Temporary	Destroy after use
	Promotion/temporary promotion/ substitution documentation	Temporary	Destroy after summary noted
	Working Time Directive opt-out forms	Short	Keep 3 years after the opt-out has been rescinded or has ceased to apply
	Record of previous service dates	Long	Keep until age 100 of data subject
	Previous service supporting papers	Temporary	Destroy after records noted as appropriate
	Qualifications/references	Medium	Keep 6 years
	Senior executive records	Long	Keep permanently
	Honours awards and nominations	Long	Keep permanently
	Transfer documents (OGD E18)	Temporary	Destroy after summary noted and actioned
	Annual/Assessment Reports	Medium	Keep 6 years

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
	Annual/Assessment Reports for last 5 years of service	Long	Keep until age 72 of data subject
	Training history	Medium	Keep 6 years
	Travel and subsistence – claims and authorisation	Medium	Keep 6 years
	Annual leave records (in some departments)	Short	Keep 2 years
	Job applications – internal	Temporary	Keep 1 year
	Recruitment/Appointment/Promotion Board selection papers	Short	Keep 2 years (brief summary 3 years)
	Building society references	Temporary	Keep 6 months
	Security clearances	Short	Keep 3 years
Health	Health declaration (consent form only)	Long	Keep until age 100 of data subject
	Health referrals – including medical reports from doctors and consultants, incl. any correspondence with BMI Health Services or, previous to that body, the Occupational Health & Safety Agency Ltd, the Civil Service Occupational Health Service or the Medical Advisory Service (MAS)	Long	Keep permanently
	Papers relating to any injury on duty	Long	Keep until age 100 of data subject
	Medical Report of those exposed to a substance hazardous to health, including:	Long	Keep 40 years from date of last entry

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
	• Lead (Control of Lead at Work Regulations 1980)		
	• Asbestos (Control of Asbestos at Work Regulations 1996)	Long	Keep 40 years after last record
	• Compressed Air (Work in Compressed Regulations 1996)	Long	Keep 40 years from date of last entry
	• Radiation (Ionising Radiation Regulations 1985)	Long	Keep 50 years from date of last entry
	Medical/Self Certificates – unrelated to industrial injury	Medium	Keep 6 years
Pay and Pension	Bank details – current only	Medium	Keep 7 years after employment has ended
	Death benefit nomination and revocation forms	Long	Keep at least until age 72 of data subject
	Death certificates	Long	Return original to provider; keep copy at least until age 100 of data subject
	Decree Absolutes	Long	Return original to provider; keep copy at least until age 100 of data subject
	Housing advance	Medium	Keep 7 years after repayment
	Marriage Certificate	Long	Return original to provider; keep copy at least until age 100 of data subject

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
	Unpaid leave periods (maternity leave etc)	Long	Keep at least until age 72 of data subject
	Statutory Maternity Pay documents	Medium	Keep 7 years
	Other maternity pay documentation	Medium	Keep 7 years
	Overpayment documentation	Medium	Keep 7 years after repayment or write-off
	Personal payroll history – incl record of pay, performance pay, overtime pay, allowances, pay enhancements, other taxable allowances, payment for untaken leave, reduced pay, no pay, maternity leave	Long	Keep at least until age 100 of data subject
	Pensions estimates/awards	Long	Retain at least until age 100 of data subject
	Record of: • Full name; • National Insurance number; • Date of birth; • Pensionable pay at date of leaving; • Reckonable service for pension purposes (and actual service where this is different, together with reason for the difference) • Reason for leaving and new employer's name (if known); • Amount and destination of any transfer value paid;	Long	Retain at least until age 100 of data subject

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
	• Amount of any refund of PCSPS contributions; • Amount and date of any Contributions Equivalent Premium paid;		
	All papers relating to pensionability, not listed elsewhere in this annex, including: Application forms; • Papers about the pensionability of other employment (including war service); • Papers about widows', widowers', children's pensions and other dependant's pensions; • Correspondence with Cabinet Office, other departments and pensions administrators, or the officer and his/her representatives (MPs, unions etc) about pensions matters	Long	Retain at least until age 100 of data subject
	Resignation/termination/retirement letters	Long	Retain at least until age 100 of data subject
	Added years	Long	Retain at least until age 100 of data subject
	Added voluntary contributions	Long	Retain at least until age 100 of data subject
	Payroll input forms – reduced/No Pay/Maternity Leave	Medium	Keep 7 years
	Bonus nominations	Medium	Keep 7 years

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
Administration	Complete Sick Absence Record showing dates and causes of sick leave	Long	Keep at least until age 72 of data subject
	SSP1 – SSP1L	Medium	Keep for last 4 - 6 years (4 years if unrelated to industrial injury)
	Papers relating to disciplinary action which has resulted in any change to terms and conditions of service, salary, performance pay or allowances	Long	Keep at least until age 72 of data subject
	Authorisation for Deputising/Substitution Allowance, or Overtime/Travel Time Claim	Medium	Keep 7 years
	Travel & Subsistence – claims and authorisation	Medium	Keep 7 years
	Advances for: • Season tickets • Car parking • Bicycles • Christmas/holidays • Housing • Health & Safety Records	Medium	Keep 7 years after repayment
	Accident report	Short	Keep 3 years
	H & S policies	Long	Keep at least 25 years and then review every 5 years

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
	Special waste records	Short	Keep 3 years
	H & S committee papers	Medium	Keep at least 7 years and then review every 5 years
	Risk Assessments	Long	Keep at least 25 years and then review every 5 years
	Environmental duty of care regulation records	Short	Keep 2 years
	Visitor logs / sign-in sheets	Short	Keep 3 months
Contractual Records	Policy records related to contracts	Medium	Keep 7 years
	Initial proposals (includes: end user requirements, list of approved suppliers, statement of interest, draft specification, agreed specification, evaluation tender, invitation to tender)	Medium	Keep 7 years
	Tender document (includes: unsuccessful tender documents, successful tender documents, background information supplied by department, internal review of tender, commissioning letter, signed contract)	Medium	Keep 7 years
	Contract monitoring/operation (includes: reports updates from contractors schedules of works, records of compliant, disputes over payments, final accounts, minutes and papers)	Medium	Keep 7 years

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
	Data sharing agreement including licences	Medium/Long	Keep 7 years from the end date of the agreement or from deletion of the data (whichever is later). Any agreement that is necessary to document the lineage or provenance of any third party data used in JNCC outputs should be kept at least 25 years and then reviewed every 5 years.
Financial Records	Bank statements	Medium	Keep 7 years
	BACS acknowledgements (includes: payments, deposits and withdrawals)	Medium	Keep 7 years
	Petty cash requests	Medium	Keep 7 years
	Trial balances & reconciliations (includes: year-end balances, reconciliations variations, published accounts)	Medium	Keep 7 years
	Journal/virements (internal)	Medium	Keep 7 years
	Audit of accounts reports	Medium	Keep 7 years
	Debtors records and invoices (includes: copies of invoices/debit notes)	Medium	Keep 7 years
	VAT records	Medium	Keep 7 years
	Purchase orders	Medium	Keep 7 years

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
	Requisition records	Medium	Keep 7 years
	Asset register (includes: Assets, equipment)	Medium	Keep 7 years
	Depreciation registers	Medium	Keep 7 years
	GIA/Corporate Plan submissions	Medium	Keep 7 years
	Policy papers related to financial management	Medium	Keep 7 years
	Records related to loss (includes records for, loss, theft, fraud, overpayments, write-offs)	Long	Keep 10 years after investigation
	Procedure manuals	Short	Keep 2 years
	Management reporting records (includes: quarterly reporting, time recording, risk reviews, performance reports)	Medium	Keep 7 years
Communications Press	Press releases	Medium	Keep 7 years
	Policies related to communications	Medium	Keep 7 years
	Reports	Medium	Keep 7 years
	Publications/Books	Medium	Keep 7 years
	Image libraries	Medium	Keep 7 years

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
Access to Information Requests	Routine FOI/EIR/RoPSI requests	Short	Keep 3 years
	FOI/EIR/RoPSI requests where there is an internal review and/or complaint to the Information Commissioner	Medium	Keep 7 years
Project Records	Project proposals	Long	Keep 10 years after completion of project
	Project management documents (includes: project plans, risk logs, issues log, project mandates/justifications, benefit reviews, product breakdowns, minutes from checkpoint meetings, project board approvals, business case)	Long	Keep 10 years after completion of project
	Feasibility studies (includes: reports, draft reports, working papers, correspondence)	Short - Long	Keep 2-10 years
Business Support	Strategy	Long	Keep 10 years
	Business Continuity	Medium	Keep 7 years
	Technical documents	Short	2 years
	Technical polices (includes: email policy, IT security policy, mobile computing policy, equipment loan policy)	Medium	Keep 7 years
Corporate Governance	Constitution, membership and committee papers	Long	Keep at least 25 years and then review every 5 years
	Relation with sponsor agencies/stakeholders	Medium	Keep 7 years

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
	Corporate vision, mission statements	Long	Keep 10 years
	Corporate annual business plans	Long	Keep at least 25 years and then review every 5 years
	Corporate annual business planning cycle records	Medium	Keep 7 years
	Project & programme reviews	Medium	Keep 7 years
	Risk Management/audit	Medium	Keep 7 years
Digital Products	Published data outputs (including open data, transparency data, and official statistics)	Long	Keep at least 25 years and then review every 5 years
	Documentation on lineage of published data outputs (including open data and official statistics)	Long	Keep at least 25 years and then review every 5 years
	Internal metadata catalogue records (including Topcat records)	Long	Keep at least 25 years and then review every 5 years
	Third-party data licensed for a fixed period	Medium	Keep 7 years from end of licensing period, subject to any contractual requirements to delete or return the data
	Third-party data licences and documentation on lineage of third-party data use	Long	Keep at least 25 years and then review every 5 years
Website	Project Board - current	Short	Keep at least 3 years
	Website content	Short	Keep at least 3 years

Electronic document group	Electronic document type	Lifecycle	Retention period and review schedule
	Site architecture	Medium	Keep 7 years and then review every 5 years
	Website design	Short	Keep at least 3 years
	Web team meetings	Short	Keep at least 3 years
	Website projects	Medium	Keep 7 years and then review every 5 years
	Web guidance	Short	Keep at least 3 years
	Training	Medium	Keep 7 years and then review every 5 years

Annex B Document Disposal Matrix

Date	Asset Name	Programme/Project	Disposal Date	Disposal Method	Reason for Disposal	Disposed By	Authorised By	Scanned	Notes

Annex C Legislation

Limitation Act 1980

The Limitation Act 1980 is a statute of limitations that establishes time limits within which action may be taken for breaches of the law. In particular this act sets out a time limit of six years for making most claims that rely on contracts and torts. Retention periods for many categories of document are set based on the potential need to defend against claims that may arise before the relevant time limit expires.

Freedom of Information Act 2000 and the Environmental Information Regulations 2004

Disposal schedules are useful for demonstrating why JNCC no longer holds information that was held previously, and can help JNCC defend against criticisms of record management practices made in complaints under the FOIA/EIR regime. In particular good documentation of decision-making on disposal of information may be crucial in refuting charges that records have been destroyed with the intention of preventing disclosure in response to an access to information request, contrary to section 77 FOIA or regulation 19 EIR.

Data Protection

Retention and disposal of personal data in JNCC records is subject to legislative requirements under the General Data Protection Regulation, the Data Protection Act 2018, and other legislation. Please refer to JNCC's Data Protection Policy for background.