ORGANISATIONS

RECORDS MANAGEMENT CHECKLIST

digital TOOLKIT

Guidance for Organisations

This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice when renewing, enhancing or developing their own processes and procedures or for specific legal issues and/or questions.

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Records Management Checklist

Records management organisation

Does your business have defined and allocated records management responsibilities?

You should assign lead responsibility for records management at a senior enough level to be able to change policy, process and culture. Where resources are available, you should nominate an appropriately skilled lead to coordinate records management within your business. You may combine this with other roles within your business.

Where resources are available, you should nominate an appropriately skilled records management lead to coordinate the management of records within the business. This may be combined with other roles within the organisation.

Records management policy

Has your business has approved and published an appropriate records management policy?

A policy will address how records are used within your business in a consistent manner. This can be part of a general policy or a standalone policy statement that is supported by specific records management procedures such as storage and maintenance or disposal of records. The policy should clearly set out:

- Your approach to records management and should address your overall commitment;
- The role of records management;
- References to related policies and documents, staff roles and responsibilities;
- Monitoring of compliance.

This should be subject to a regular review process and changes made as necessary.

Records management risk

Has your business identified records management risks as part of a wider information risk management process?

You should carry out regular exercises to identify, assess and manage records management risks. This review should identify what could go wrong with a process and how this might happen. Once you know what the risks are, you can then put measures in place to mitigate these risks.

If you already have a corporate risk register, you can use this to include risks to records management functions. These might include records not being either updated, destroyed in a timely manner or held securely.

Records management training

Has your business incorporated records management within a formal training programme?

This should comprise compulsory induction training for new starters and regular refresher material. Specialist training should also be provided for those with specific records management functions.

You should brief all new staff on their responsibilities for the creation, use, maintenance and eventual destruction of records with regular refreshers to maintain levels of awareness. Awareness materials might include posters, office-wide emails, intranet updates and records management content in newsletters. You should give specialist training to staff with specific records management responsibilities such as management of disposal schedules, monitoring of data quality or oversight of records management practice in order to allow them to carry out their role effectively.

Staff should be aware of what they can/cannot do with an organisation's records and who has responsibility for what.

Monitoring and reporting

Has your business carried out periodic checks on records security and is there monitoring of compliance with records management procedures?

Performance measures might include progress against a records management action plan, archive retrieval rates measured against a service level agreement (SLA), progress regarding deletion of records against requirements of a retention schedule or data quality and accuracy. You should report on performance to key performance indicators (KPIs) periodically to management to provide assurances on compliance.

Records creation and maintenance

Record creation

Has your business set minimum standards for the creation of paper or electronic records?

You should ensure you have procedures and guidelines in place for referencing, titling and indexing new records. You should also implement a 'security classification' scheme where possible so that you can classify or mark new records according to their sensitivity. This will help you control access to those records (ensuring that the only people who can access those records are those with a genuine business need) and allow for efficient management, retrieval and disposal.

Although emails are often perceived differently to other records, they still contain information which has a wider business purpose as well as personal data, so you should manage them in a consistent way.

Information you hold

Has your business identified where you use manual and electronic records keeping systems and do you actively maintain a centralised record of those systems?

In order to ensure that personal data is managed effectively and securely, you need to know what information you hold and how it is held. You should carry out an information audit or records survey to identify the records and data sets you hold. This will help you to catalogue the data that you process and how it flows into, through and out of your business.

It will also help you determine which business functions create certain records, which records are vital to your business, where you keep them, how long you keep them for and who needs to use them now and in the future.

In order to gather the information you need as part of the information audit you could distribute questionnaires to key people in all areas or roles of your business.

You should document your findings, for example in an information asset register.

These findings may allow you to develop retention and disposal schedules, improve security practices, and aid the development of disaster recovery processes.

Information standards

Has your business got processes in place to ensure that the personal data you collect is accurate, adequate, relevant and not excessive? Do you carry out regular reviews to remove any personal data or records that are out of date or no longer relevant?

You should ensure that you take reasonable steps to safeguard the accuracy of the personal data you collect and deal with challenges to its accuracy from individuals about whom you have recorded information.

You should have processes in place to ensure that you remove personal data which is inaccurate or out of date from records on a regular basis. This will enable you to amend, remove or clarify personal data you hold when appropriate.

Data you collect, store and process should be adequate, relevant and limited to what is necessary. If you do not make decisions about what personal data you should hold for your business purposes then you are at risk of collecting excessive data and infringing the privacy of an individual, or you may hold too little to make effective decisions about those individuals. What is adequate, relevant and not excessive will change with your business needs over time and you must regularly review and check that you are not collecting more than is necessary for your business needs.

Under the DPJL, individuals have the right to have their personal data rectified if it is inaccurate or completed if it is incomplete. You should have appropriate systems in place to deal with individuals' requests to correct or complete information, or to allow individuals to provide a supplementary statement.

You need to have processes in place that enable you to restrict personal data if required. You should use methods of restriction that are appropriate for the type of processing you are carrying out.

There are a number of different methods that you could use to restrict data, such as:

- Temporarily moving the data to another processing system;
- Making the data unavailable to users;
- Temporarily removing published data from a website.

It is particularly important that you consider how you store personal data that you no longer need to process but the individual has requested you restrict (effectively requesting that you do not erase the data).

If you are using an automated filing system, you need to use technical measures to ensure that you cannot carry out any further processing or change the data whilst the restriction is in place. You should also note on your system that the processing of this data is restricted.

Tracking and offsite storage of paper records

Has your business got tracking mechanisms in place to record the movement of manual records and ensure their security between office and storage areas and also in instances where records are taken off-site?

Your employees may need to take paper records off-site in order to work remotely, e.g. to visit service users or to attend court hearings. You may also wish to store archived records off-site due to limitations on office space.

You should have procedures in place to ensure that you know what records are off-site and who is holding them so you can recover them if necessary or destroy them when they reach the end of their retention period.

When transferring data off-site, you should minimise it, use an appropriate form of transport, e.g. secure courier for sensitive personal data, log the transfer in and out where appropriate and put checks in place to ensure that data is received. Security measures which you could use include lockable containers, tamper evident packaging, and removal from public view and accessibility.

Effective tracking of manual records will also help you to locate and retrieve information quickly should you receive a subject access request.

Offsite transfer of electronic records

Has your business got appropriate measures in place to transfer electronic records off-site and protect personal data from loss or theft?

You may transfer personal data off-site using electronic means such as email or removable media e.g. USB sticks or DVDs. CDs, DVDs, USB drives, smartphones and tablet devices are vulnerable to theft or loss.

If there is a business need to transfer personal data via email or removable media, you should try to minimise the amount of information being transferred and either send it by encrypted mail or use secure devices which have been encrypted to protect unauthorised access to the data they hold.

You should use an appropriate form of transport e.g. secure courier for sensitive personal data. You should log the transfer in and out where appropriate and check that data is received.

Security measures which you could use include tamper evident packaging, encrypted devices, or encrypted emails or secure file sharing or transfer software.

Secure storage of records

Does your business store paper and electronic records securely with appropriate environmental controls and higher levels of security around special categories of personal data?

You should use lockable offices, cabinets and drawers to store records, with higher levels of security for records containing special categories of personal data. You should also store keys securely and lock records away when staff are absent for extended periods, e.g. overnight.

Employees should lock screens when away from their desks to avoid unauthorised and untraceable access, theft, destruction or alteration of data.

Environmental controls for records storage areas might include waterproofing and drainage to protect against flood risk, fire protection such as use of fire resistant or fireproof materials, fire control systems and heating to protect against damp.

There are an increasing number of services offering cloud storage where you can upload your documents, records and other files. You need to check that the security and availability of the service is right for you. Think carefully about who can access your records and the location of the servers that are storing your data, check the storage provider's terms and conditions and privacy notice and try to encrypt your data before placing it in the cloud.

Access to records

Does your business restrict access to records storage areas in order to prevent unauthorised access, damage, theft or loss. You should implement role-based access and check it regularly?

In order to reduce the risk of unauthorised access you should consider who needs access to what personal data in order to fulfil their function. For example, it is likely that only specific members of staff would need access to HR records. In such cases, you should limit access with keys, swipe cards, pin codes or other security measures.

Does your business have a process to assign and manage user accounts to authorised individuals and to remove them when no longer appropriate?

Management should authorise access to systems holding personal data and ensure permissions are restricted to the absolute minimum (known as 'least privilege'). Each user should be assigned their own username and password to ensure accountability and that there is an audit trail.

You should review access permissions periodically to ensure the privileges granted continue to be based on business need and have been correctly authorised. The frequency of review will depend on the level of privilege granted to the user and the type of information they have access to.

You should also monitor user activity to detect any unusual use (including sending information out of the organisation). Passwords should not be shared and passwords should be promptly disabled when a user changes duties or leaves the organisation.

Business continuity

Does your business have appropriate business continuity plans in place in the event of a disaster?

This includes identifying records that are critical to the continued functioning or reconstitution of your business. You also routinely back up data that is stored electronically to help restore information if needed.

You should have a plan for how you would deal with serious disruption to your business and this should be communicated to all staff. All staff should know what to do in the event of a serious disruption.

You will hold data which you cannot function without. You should therefore assess the data you hold and identify how critical it is to the functioning of your business.

You should make regular backups so that you can restore personal data stored electronically in the event of disaster or hardware failure. The extent and frequency of backups should reflect the sensitivity and confidentiality of the personal data, how critical it is to the continued operation of your business. Ideally you should store backups off-site.

Disposal of data

Does your business have a retention and disposal schedule which details how long you will keep manual and electronic records?

You should keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes you are processing it. You should identify what types of records or data sets you hold, what type of information these records hold and then destroy, delete or anonymise personal data within records you hold as soon as it becomes surplus to requirements.

Once you have completed a records survey, you can assign retention periods to records and data sets. You can then destroy records once they reach the end of this retention period.

Does your business have confidential waste disposal processes in place to ensure that records are destroyed to an appropriate standard?

You can destroy paper records in a variety of ways including micro-cut shredding or incineration. Your method of destruction should match the sensitivity of personal data being destroyed and you should carry out checks to ensure that staff are complying with the procedures. You should also be able to delete electronic records from systems, however if this is not technically possible, you should 'put them beyond use'.

Where every day confidential waste is awaiting disposal, you should store it securely, for example in lockable confidential waste bins. You may require larger storage areas for disposal of large amounts of personal data.

In addition, under the DPJL individuals have the right to request that you erase their personal data – this is known more commonly as the right to be forgotten. An individual can request to have their personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws consent and there is no other legal ground for the processing;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing (including objecting to direct marketing);

- The personal data has been unlawfully processed (i.e. otherwise in breach of the DPJL);
- The personal data has to be erased in order to comply with a legal obligation;
- The personal data is processed in relation to the offer of information society services to a child.

The request may fall outside your standard destruction schedule. You should have processes in place to allow you to action any individual requests.

This is not an absolute right and you do not have to erase the requested information if you still have a lawful need to keep it (e.g. you need to hold on to it for accounting purposes or to deal with a legal claim).