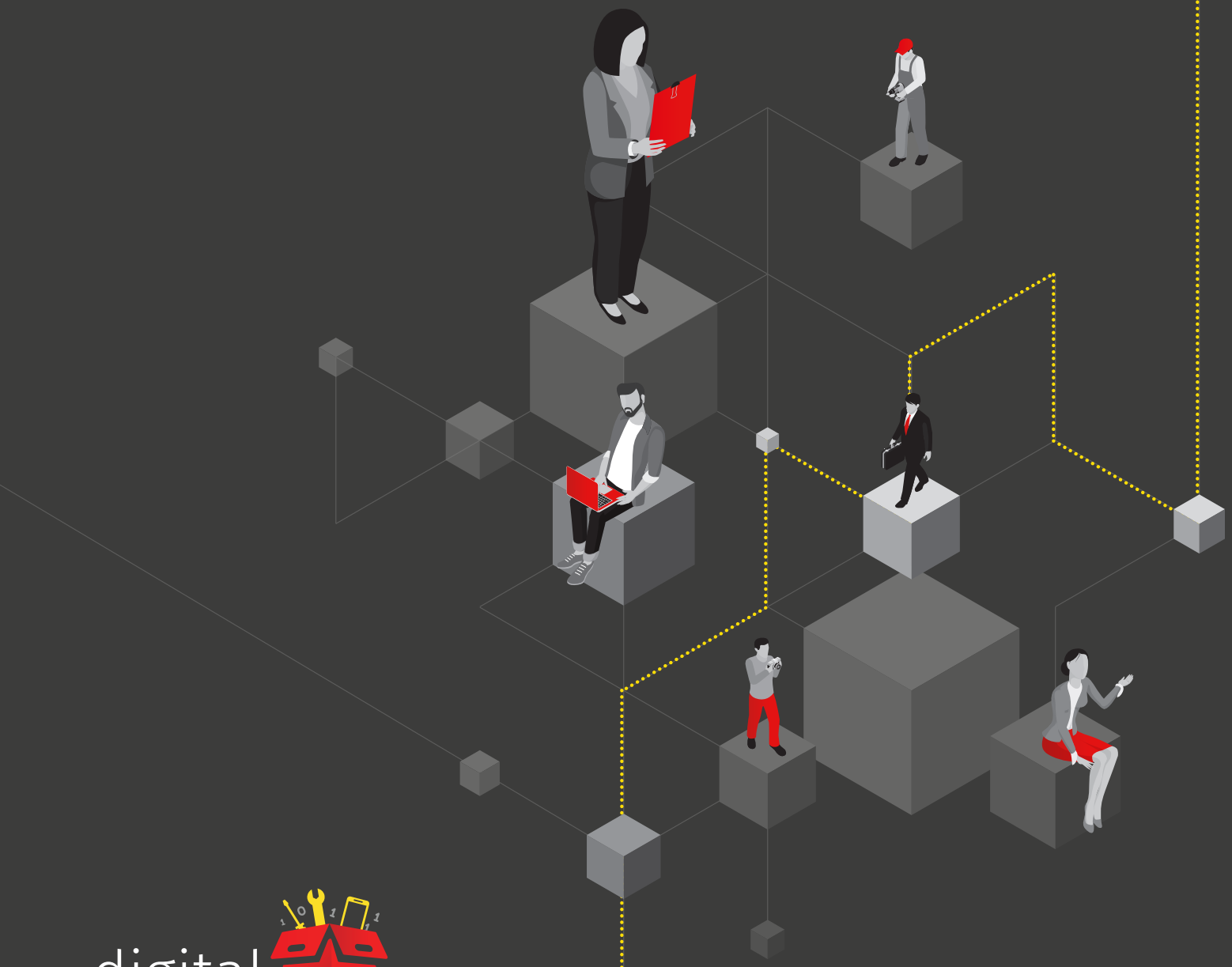
ORGANISATIONS

RECORDS MANAGEMENT **CHECKLIST**



digital **TOOLKIT**

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Records Management Checklist

Data Protection affects many areas within every organisation, no matter how large or small. To ensure you are operating within the Data Protection (Jersey) Law 2018 (**DPJL**) here is a checklist to help you navigate your organisation's approach to records management.

In short, the key things you should know are: what information have you got, why have you got it, where is it held, how long are you keeping it for and who has access to it?

You should be able to answer each of those questions so that you can advise data subjects about how their information is being used by you.

Having a good records management policy and procedure has many benefits for your organisation including increasing trust between you and your customers and ensuring that you are compliant with the DPJL.

Records management policy:

Write out a brief statement and action points which concisely reflects your approach to records management. This is a simple go to document to make sure that everything else you do relates to the records you use everyday aligns with your simple records management aims and is consistent with your privacy policy and other data protection documentation. For example:

- We ensure that all electronic and paper records are kept safe at all times;
- We ensure that we follow our retention plan;
- We understand what records we use, where we keep them and how we use them;
- Reflect back to your privacy policy.

You should review your records management aims regularly to make sure they are working for you and truly reflect your business and its activities. Everyone in your organisation needs to know what they need to do to help you achieve your compliance aims.

Records management risk:

Identify records, which you understand pose a risk to your business, such as staff health information, access codes etc. Understanding risk means understanding the potential harm to data subjects if their information is lost, stolen or otherwise compromised: what is the worst that could happen to the data subjects e.g. could someone steal their identify or use their banking details to make fraudulent purchases. Once you know the risks involved, this will help you identify what steps you need to take to ensure (insofar as you can) that the information you have remains safe and secure.

Records management training:

If you have staff you will need to incorporate data protection and records management within any induction training programme and then offer periodic updates to ensure that staff remain aware of your organisation's data protection responsibilities and can help you with your compliance. You need to keep a record of what training you provide (when, content etc.) and who attends it. You might want to give certain key members of staff (e.g. those with particular responsibility for records management) more advanced/intensive training depending on their role.

Periodic checks:	Carry out periodic checks on records security to make sure what you think is happening really is happening with the records and personal information you are using.
Record creation:	Set up a simple set of minimum standards for the creation of paper or electronic records.
Information you hold:	Know the information you hold. Follow our simple guide; 'How do we document what and how we use **personal information**'.
Information standards:	You will need to ensure that the personal data you collect is accurate, adequate, relevant and not excessive for your organisation's needs. Only collect what you need.
Tracking of paper records and transfer of electronic records:	Establish simple and proportionate tracking mechanisms to record the movement of manual records and ensure their security between where they are normally kept and if they are moved. Consider the security, risk and accessibility of any movement of records outside of your physical or electronic filing system. Make sure staff know what to do if something happens (e.g. they lose them/they are stolen).
Secure storage of records:	You must ensure that all personal information is kept securely with appropriate controls and higher level security around special categories of personal data. (**Special category data** means information that is more sensitive including that relating to health, sexual orientation, and criminal convictions. See our separate note).
Access to records:	Restrict access to records to only those individuals who need to access it for legitimate work purposes – consider implementing a role based access and check it regularly. Have a process to assign and manage user accounts to authorise individuals and to remove them when it's no longer appropriate for them to have access e.g. they leave or move to a different role.
Business continuity:	Evaluate and document practical business continuity plans in the event of a disaster; including identifying records that are critical to the continual functioning or reconstruction of your business. You should also routinely back up data that is stored electronically so that you can restore information when needed.
Disposal of data:	Establish a retention and disposal schedule which details how long you will keep manual and electronic records and the trigger points for their destruction. How long do you want to keep information for? Why do you need to keep it for that long? (Some information may not need to be kept as long as other pieces of information.)
Disposal of data:	Have a confidential waste disposal processes to ensure that records are destroyed to an appropriate standard and make sure that your staff dispose of information in an appropriate way e.g. using a cross cut shredder rather than putting it in the standard rubbish bin.

Jersey Office of the Information Commissioner, 2nd Floor, 5 Castle Street, St Helier, Jersey JE2 3BT
Telephone number: +44 (0) 1534 716530 | **Email:** enquiries@jerseyoic.org