DATA PROTECTION
TOP TIPS

digital
TOOLKIT

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

NEW TO DATA PROTECTION?

These top tips have been designed to introduce you to the spirit of our local Data Protection (Jersey) Law 2018 and help you get started.

What is Data Protection?

Data Protection is about the fair, transparent and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations (such as sole traders, businesses, charities, clubs and associations). It's also about treating people fairly and openly whilst recognising their right to have control over their own personal data.

Why is Data Protection important?

Protecting and caring for people's personal data is vital to protect their privacy and in turn, their wellbeing. It's also a legal requirement under the Data Protection (Jersey) Law 2018 (that's our local version of the European General Data Protection Regulation, also known as the 'GDPR'). Data protection is about ensuring people can trust you to use their personal data fairly, responsibly and in accordance with the law. If you don't look after this information properly, and something happens (e.g. the information is lost or stolen) this can have significant effects for individuals. It can also put your organisation at risk of complaints and investigative action from our office.

Who needs to comply with the Jersey Data Protection Law?

All those who use information about individuals for any reason other than their own personal, family or household purposes, need to comply with the law. The law takes a flexible, risk-based approach which encourages those that use (for example, collect, record or store) people's personal data, to think carefully about how and why they need it, use it and for how long they need to keep it. You need to make sure you look after that personal data and keep it safe and secure and that only the right people in your organisation have access to it.

Using Personal Data:

- Think ‘data protection’ from the moment you collect customer, volunteer, staff, member or supplier personal data. It’s easier to protect than correct!
- Know and make sure you can explain to individuals:
    - » what you are collecting
    - » why you need it
    - » how you are using it
    - » what measures you have in place to keep it safe
- Only process what you really need. Information minimisation reduces risk.
- Treat all personal data with the same respect and security as you would wish for your own personal data.
- Carefully consider who, how, what and why you need to share personal data before doing so. If it is not necessary to do so, then don’t.
- Make sure that you are transparent about how you are using people’s personal data. Most organisations use something called a privacy policy/data protection statement to give this information to individuals and many post it on their website. If you don’t have a privacy policy, create one using our handy template. It’s a legal requirement to be open with individuals about how you’re using their information.

People and Data Protection:

- Train, train, train. Data protection training and awareness for all staff, volunteers and executives is fundamental. They need to know what they can/cannot do with the information entrusted to them and what to do if something happens so they can support your organisation to maintain the highest data protection standards.
- Check who has access to personal data to ensure that only those who need access, have access.

Managing Personal Data:

- Consider turning off the ‘auto-complete’ function for email addresses. How many times have you mistakenly sent an email to the wrong person? (Remember this may be a personal data breach under the law and may be reportable to our office.)
- Use the BCC field when sending emails to more than one recipient. Avoid the risk of sharing personal data with someone who shouldn’t have it.
- Think twice before forwarding emails as they may contain information from previous correspondence that shouldn’t be shared.
- Take extra care to protect and secure sensitive information, such as medical, racial, ethnic, religious or criminal record details.
- Take care not to leave paperwork containing personal data in view of others.

Storing and Assessing Personal Data:

- Keep a personal data breach log and make sure it's kept up to date. Review it regularly to identify if there is a pattern of breaches that need to addressed. Consider if any breaches need to be reported to our office.
- Make sure that any IT security / software updates are implemented in a timely manner.
- Finally – only keep personal data for as long as it is necessary and safely destroy it when it is no longer required.

Always remember that we want you to be data protection confident. If you're in doubt and not sure about something related to data protection, have questions, or need advice, our team at the Jersey Office of the Information Commissioner is available to help you. You can call us on 716530, email us at enquiries@jerseyoic.org or visit our dedicated resource room at www.jerseyoic.org that includes a variety of handy toolkits, checklists, templates and how-to-guides.

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