EAST RIDING
OF YORKSHIRE COUNCIL

Data Protection and Security

Training Booklet v1.7a

Contents

Welcome

Welcome to this training booklet on Data Protection (launched May 2018). The training outlines how to treat information securely to comply with legislation and our policies.

All Council employees are required to undertake some form of data protection training (data protection compliance indicator). If you are unsure which training you should be completing please read the Council's Data Protection Training Procedure (available on the intranet).

You can only use this booklet to achieve your Data Protection compliance indicator if you do not have network access or regular access to personal data.

Once you have done this, please return the completion slip and return it to the Training Section at eryctraining.support@eastriding.gov.uk or to the following address:

Learning and Development Support Services
The Hexagon Centre
Coltman Avenue
Beverley
HU17 9LP

Section 1 - Introduction

Data Protection

The Data Protection Act 2018 (DPA) replaces the Data Protection Act 1998. It is an Act of Parliament of the United Kingdom which controls how personal data is used and that it is protected.

It is an important piece of legislation giving confidence to individuals that their personal data will be treated appropriately and that it will not be misused.

The council and its staff have a duty to protect data and treat information securely, that means each and every one of us.

What is the Purpose of the Data Protection Act?

The Legal Stuff

The 2018 Data Protection Act was updated following a new European Union Regulation, the General Data Protection Regulation (GDPR). Because GDPR is a regulation it is automatically applied in all EU member states from the 25 May 2018. As the UK was part of the EU at the time and helped develop GDPR it was a law the government was keen to see updated.

The new Data Protection Act was needed to support implementation of the Crime Directive. The Crime Directive, unlike GDPR, did not automatically apply in all EU countries. The Crime Directive was needed as it covered personal data in relation to crime and enforcement, something which the GDPR did not include. The GDPR also included a number of derogations (areas where the UK government could make its own choices); the Data Protection Act 2018 implements these derogations.

What it really means

Data Protection law reinforces common sense rules regarding information handling which most organisations, including East Riding of Yorkshire Council, try to follow anyway. It is there to ensure that we manage personal information in a sensible way and treat our customers and their information with respect.

Consider how you would like your personal information to be treated and then think about how you treat the information you handle relating to others.

Don't Forget

The council holds a significant amount of personal data about each and every one of us! If you live in the area you probably pay council tax; you may be a housing tenant; how about membership at the leisure centre?

Even if none of these apply, you are certainly an employee which means payroll and HR records are held as a minimum.

Role of the Information Commissioners Office

The Information Commissioner's Office (ICO) is a UK independent body responsible for upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Under the requirements of the Data Protection Act, businesses and organisations that handle personal data must register with the ICO as Data Controllers, unless they're exempt.

The council is registered with the ICO; Elected Members and Schools are registered separately.

Part of the role of the ICO is to take action to ensure we meet our information rights obligation. This includes monetary penalties and fines, enforcement notices and other actions including criminal prosecutions we may be subject to. In addition to the Data Protection Act, the ICO enforces and oversees:

- The Freedom of Information Act
- The Privacy and Electronic Communications Regulations
- The Environmental Information Regulations
- INSPIRE (spatial information)
- Reuse of public sector information regulations.

Data Protection Headlines

Data Protection is often in the news; let's make sure East Riding of Yorkshire Council stays out of the headlines.

Section 2 - Definitions and Principles

Data Protection Definitions

There is often confusion surrounding the terminology used in the Data Protection Act. To eliminate some of the confusion the following is a list of the common words and phrases applied in the act.

Personal Data

Any information about a living individual who can be identified from the data stored by the Data Controller. **Remember**…..Voice and image (recordings, photos, CCTV, online identifiers etc.) are also considered to be Personal Data if the individual can be identified.

Special Category Data

Special Category Data is personal data revealing the following:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or similar beliefs
- Trade union membership
- Physical and mental health conditions
- Sexual orientation
- Genetic information
- Bio-metric information

Law Enforcement Data

Personal data for the purposes of prevention, detection, prosecution of criminal offences or the execution of criminal penalties including safeguarding against threats to public security.

Processing

The definition of processing is very wide and it is difficult to think of anything an organisation might do with data that will not be processing.

- Obtaining or recording the data
- Storing the data

- Organising, adapting or altering the data
- Retrieving or making decisions based on the data

Data Controller
The person or organisation who holds the information and determines the lawful purposes for which the data is processed and disclosed i.e. East Riding of Yorkshire Council - Us!

Data Processor
Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Subject
The individual who is the subject of the personal data - a living individual.

Profiling
Any automated processing of personal data to evaluate, analyse or predict personal aspects relating to performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location and movement.

Pseudonymisation
Removing identifiers from information, leaving a key/reference so they can be matched back at a later date.

Data Protection Principles

There are 6 core principles governing the use of personal information which we must comply with. In addition there is also a requirement to demonstrate compliance with the 6 principles.

Lawfulness, fairness and transparency**:** Personal data shall be processed lawfully, fairly and in a transparent manner.

Purpose limitation**:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Purpose limitation**:** Personal data shall be adequate, relevant and limited to what is necessary.

Accuracy**:** Personal data shall be accurate and, where necessary, kept up to date.

Storage limitation**:** Personal data shall be kept in a form which permits identification for no longer than is necessary

Integrity and confidentiality**:** Personal data shall be processed in a manner that ensures appropriate security, including unauthorised or unlawful processing and protection against loss or destruction/damage.

The principles are in essence a code of good practice for processing personal data. They are the 'backbone' of the Act. Further information can be found at the Information Commissioner's Office website.

Section 3 - How We Use Information

The council holds and processes lots of personal information daily. We receive information from many sources, including other public agencies and also produce a huge variety of information.

Conditions for Processing

If you process personal information it must be done under Conditions for Processing. It's important you understand on what grounds you are processing personal data as this affects the rights people have (covered in section 4).

Personal data

If you are processing personal data it can be done under the following conditions.

- Consent
- Performance of a contract
- Legal obligation
- Vital interest
- Public interest
- Legitimate interest.

As a council we should try and apply performance of a contract, legal obligation and public interest.

Special category data

If you are processing special category data the conditions for processing are different.

- Explicit consent
- Employment and social security and social protection law
- Vital interest
- Legitimate activities
- Made public by the data subject
- Legal claims or whenever courts are acting in their judicial capacity
- Substantial public interest

Preventative or occupational medicine/provision of health and social care

Law Enforcement Data
If you are processing law enforcement data the conditions for processing are different.

- Judicial and statutory purposes
- Protecting individual's vital interests
- Personal data already in the public domain
- Legal claims
- Judicial acts
- Preventing fraud
- Archiving

The council has a number of policies which cover Data Protection and Information Security. Everyone who works for us, or with us and who handles our information, or uses our facilities, must act in accordance with these policies.

You have a responsibility to make sure you are familiar with the Data Protection Policy. You can ask your manager for a copy or search the Intranet.

Below is a list of additional East Riding of Yorkshire Council policies and guidance documents (some of them are still under review). You can access them on the Intranet. Try and familiarise yourself with them all.

- ICT Computer Usage Policy
- Data Protection Incident and Breach Procedure
- Data Protection Request Procedure
- Data Protection impact Assessment Procedure
- Data Protection Training Procedure
- Redaction Guidance
- Clear Desk and Screen Guidance
- Humber Information Sharing Charter
- Records Management Policy

Data Protection Officer
The council is required to have a data protection officer (DPO). The DPO is responsible for overseeing this area and ensuring privacy is at the forefront of council business.

The Council's DPO is Mathew Buckley, Head of Legal and Democratic Services. To contact the DPO email data.protection@eastriding.gov.uk or phone (01482) 391419.

Information Asset Register (IAR)

The Council is required to hold detailed records of processing (these are our information asset registers). They are required to show the following information and are used by the ICO to hold us to account.

- What information we hold
- How long we hold it
- Under which condition we process the data
- Who we share it with
- Who has access (security)

You can find your service IAR on the intranet.

Privacy Notices

When you collect information that relates to living individuals, you must tell people what you are going to use their personal information for.

This is done via a Privacy Notice (sometimes known as a Fair Processing Notice).

The Council makes every effort to ensure the way in which it uses data is transparent, fair and lawful. As part of this it has a section of its website dedicated to privacy, this includes a privacy notice directory for all council services. It can be found at – www.eastriding.gov.uk/privacynotice.

This would need to include:

- Who you are
- Why you are using the data and for what purpose
- Who you are sharing it with
- If you are transferring it outside of the country
- How long you are holding it for
- What rights people have
- The fact they can complain
- The Data Protection Officers contact details
- Details of any automated decision making

Consent

If you are relying on consent as the basis for processing personal data then your consent must be:

- Opt in
- Clear

- Informed
- Freely given
- Auditable

Consent must be a choice and people must be able to withdraw it. If consent is relied upon it also means that everyone of their rights in respect of personal data applies (section 4 covers people's rights). Ideally the council should use consent as a last resort. If it is withdrawn this could cause problems later down the line.

If children are using information society services (online services) parental consent is required for those aged under 13. The best way of ensuring you have valid consent is to make sure you have a valid Privacy Notice. Detailed guidance is available on the Intranet.

Section 4 - Rights

Data Subject Rights

People (data subjects) have a number of rights in respect of their personal data. You need to be aware of the rights individuals have in order to be prepared should someone contact you, most rights have a one month timescale (28 days to ensure compliance).

Right to rectification
People can ask for their information to be rectified if it is inaccurate or incomplete. Before any information is updated we would need confirmation and evidence from the individual.

If the information which is inaccurate or incomplete has been shared with anyone else, you would also need to contact them and let them know.

Right to erasure
The right to erasure is often referred to as the right to be forgotten. This right enables people to ask for information to be deleted or removed in certain circumstances; it does not give them the right to have anything they want deleted.

Right to restrict processing
Under this right the council is permitted to store the information, but not further process it effectively blocking its use.

This right applies if:

- An individual contests the accuracy
- An individual objects to the processing and the council is considering the objection
- When processing is unlawful
- When you no longer need the information but the individual wants you to keep it.

Right to portability
This right allows people to transfer their data from one IT system to another similar to a Subject Access Request, but business to business. It only applies if personal data has been provided to the council. Processing is based on consent or performance of a contract when processing is carried out by automated means.

Right to object
This right allows the council to stop processing personal data.

It only applies if:

- Processing is based on legitimate interest or public interest
- Carrying out direct marketing
- Processing for scientific/historical research

If somebody objects you must stop processing immediately. If you can demonstrate compelling grounds for processing which override the interests, rights and freedoms of the objector, or if the processing is being used for defense of legal claims then you can continue processing data.

Automated processing
Rights related to automated decision making and profiling. For something to be solely automated there must be no human involvement. The decisions made must have a negative impact on the individuals.

Individuals also have the right to object to profiling and ensure that people can obtain human intervention and an explanation of how the decision was made.

Right of Access
People can request to see information we hold about them by submitting a 'Subject Access Request'. A request of this nature only has to be in writing it doesn't have to be on a specific form. It is your job to recognise if someone is making a request.

If you receive a request for information, you must **immediately** pass it on to the Data Protection Team.

You can send an email to data.protection@eastriding.gov.uk so that they can deal with the request promptly.

What Happens to the Request?
All valid requests will be given a reference number e.g. SAR123. This includes checking the identity of the person making the request.

Requests are free of charge and must be completed within one month (28 days). In certain circumstances, mainly large complex requests, they can be extended by a further two months (56 days to ensure compliance); this can only be done by the data protection team.

Can a Request Be Made About Someone Else?
A request for information about somebody else is not permitted unless they are authorised to do so, such as consent or power of attorney. The council has a procedure for dealing with these types of request.

There are circumstances in which you may get asked to share data about people by other organisations. These could be for example to prevent or detect crime, for the assessment of tax or to prevent harm. It is the responsibility of employees to ensure that they have the authority to share information and that the recipient is authorised to receive the information. These types of requests need to be logged and a record kept of what is released, to who and why. If you're unsure always ask.

Can I Access Personal Information About My Child?
Information about children may be released to a person with parental responsibility, the best interest of the child will always be considered.

If a child is very young, data about them is still their personal data and does not belong to anyone else. It is the child who has a right of access to the information held about them. The council usually seeks consent from any child over the age of 12 before releasing information to parents.

Consideration would be given to whether or not the child understands (in broad terms) what it means to make a request and how to interpret the information they would receive.

Redaction

What is Redaction?
Redaction is the removal of non-disclosable information. This plays a key part in responding to any Subject Access Request and can be done both using a special redaction pen or electronically to block out individual words, sentences or paragraphs or even the removal of whole pages or sections.

Why is this Important?
Supplying un-redacted documents can have serious consequences for the individual and the council. On the other hand over zealous and unnecessary redactions result in people being denied the information they have a right to. Both can result in action from the Information Commissioner's Office (ICO).

As well as redaction, the following help reduce the risk when sharing information:

Anonymisation
Involves de-identifying the data either by removing any obvious personal identifiers or by aggregating data so that only tables or totals are provided.

This might include:

- Removing names addresses etc.
- Replacing date of birth with an age band
- Providing only a partial postcode
- Reducing length of time to a time band e.g. <2 years, >5years
- Removing data that are not relevant to the analysis to be undertaken

Pseudonymisation
Attaches a coded reference (pseudonym) to each record so that they can be associated with a particular individual without that individual being identified.

Data Protection Impact Assessments

One of the ways the Council ensures people's rights are protected is by implementing privacy by design. The Council is required to implement privacy by design, this means that privacy should be at the forefront of all of our decision making.

One of the ways we do this is by carrying out data protection impact assessments. We are required to carry these out by law for high risk and large scale processing. They are considered best practice for any significant change of the way we process personal information and one of the best ways in preventing issues and penalties later down the line.

To help you decide if you need to do a DPIA you should complete the Councils screening form. For more information check the councils Data Protection Impact Assessment Procedure.

Section 5 - When Things Go Wrong

Data Protection Incident and Breach Procedure

If personal information is accidentally, unlawfully destroyed, lost, altered or accessed, this would be considered a data protection breach. At the point we think something may have occurred but is not confirmed it is considered a data protection incident.

What do I do?

As soon as you become aware of an incident or breach it must be reported to the Data Protection Team at data.protection@eastriding.gov.uk, ext: 1419.

If it involves IT it must be reported to the ICT service desk http://servicedesk/, ext: 4444.

If it relates to building security contact Infrastructure and Facilities, ext: 5990.

The council is required to report certain data protection breaches within **72 hours**. This 72 hours starts when you (the council) find out, so you must act quickly. A reporting form is on the intranet, it captures all of the information we need to make a decision on whether or not the breach is reportable.

The council also needs to report breaches to individuals who have been affected.

The council has procedure in place to make sure both of these things happen and to manage any breach. Data protection breaches not only impact upon the individual but can damage the reputation of the council. This procedure is not about getting staff in trouble; its focus is on identifying risks and preventing breaches reoccurring, by doing this it actually helps protect staff.

Some common examples that occur are:

- Leaving confidential papers/IT equipment in cars
- Breaching policy - Letting someone borrow your laptop
- Not destroying confidential waste correctly
- Security - Someone to tailgate through the secure entrance at a Council building

- Sharing information – that has been collected for one purpose but used it for another
- Email security – ensuring emails are sent to the correct recipients
- Inappropriate use of information – using Council information for personal use
- Mobile working – overheard conversations, screens being visable

The Consequences

The ICO have a number of powers they can use if the council is found to be in breach of the data protection act these include:

- Enforcement notices (forcing the Council to change processes)
- Fines up to £17 Million (€20 million)
- Audits

The potential fines are substantial (these can be issued for simple things such as lost memory sticks/CDs). Data processors are also liable for fines, they also have to report breaches and the ICO can contact them direct.

Criminal Offences

The ICO has the power to take action against the poor behaviour of individuals.

It is a criminal offence to knowingly or recklessly obtain, disclose or procure personal information. For example using information available to you at work for personal reasons or disclosing personal information to others who are not entitled to see it.

If a person has obtained information illegally, it is also an offence to sell it or offer to sell it.

It is an offence for a person knowingly or recklessly to re-identify data that was de-identified.

It is an offence to alter personal data to prevent its disclosure if the person was entitled to receive it in the first place.

Section 6 – Summary

Why does data protection matter?
Data protection matters because:

- We must abide by the laws that govern how personal information is used, this includes ensuring it remains secure

What is the Council's policy?
The council's policies outline how information should be handled in order to protect data.

How should I handle information?
You must:

- Manage information appropriately
- Keep confidential information secure
- Not carry out illegal, libellous, immoral or offensive activities
- Use your council access and identity in a way which is consistent with your role

What happens to information?

- We ensure information is processed in line with the 6 data protection principles. These act as a basic checklist for how you use personal information
- Information that we hold is stored and accessed for legitimate business reasons
- Following statutory and recommended minimum retention periods, information is destroyed and disposed of
- You only share information if you are confident you are permitted to share it.

Protecting Information

- Data protection is all about risk management
- Always report breaches so risks can be identified

Refreshing your Training
In line with Council policy you will be required to renew your knowledge of the Data Protection Act in 2 years' time.

Further Information
Information is available on the Data Protection pages of the Intranet or for Data Protection enquiries; you can contact your Data Protection & Feedback Team (ext 1419).

For more detailed information about our legal requirements under the Data Protection Act look at the ICO web site www.ico.gov.ukhttp://www.ico.gov.uk.

Finally if you are unsure - **Just Ask!**

Notes Page

Notes Page

Notes Page

Data Protection and Security Training Booklet Confirmation

Please use the *Confirmation of Completion and Evaluation* eForm on ASC LeadER to let us know you have completed this Module

- For East Riding Employees – your Learning Record will be updated to show that you have completed this learning.
- For Shared Lives Carers – your Shared Lives Learning Record will be updated to show that you have completed this learning.
- For Independent Care Sector workers – a Certificate will be emailed to your Line Manager to confirm you have completed this learning.