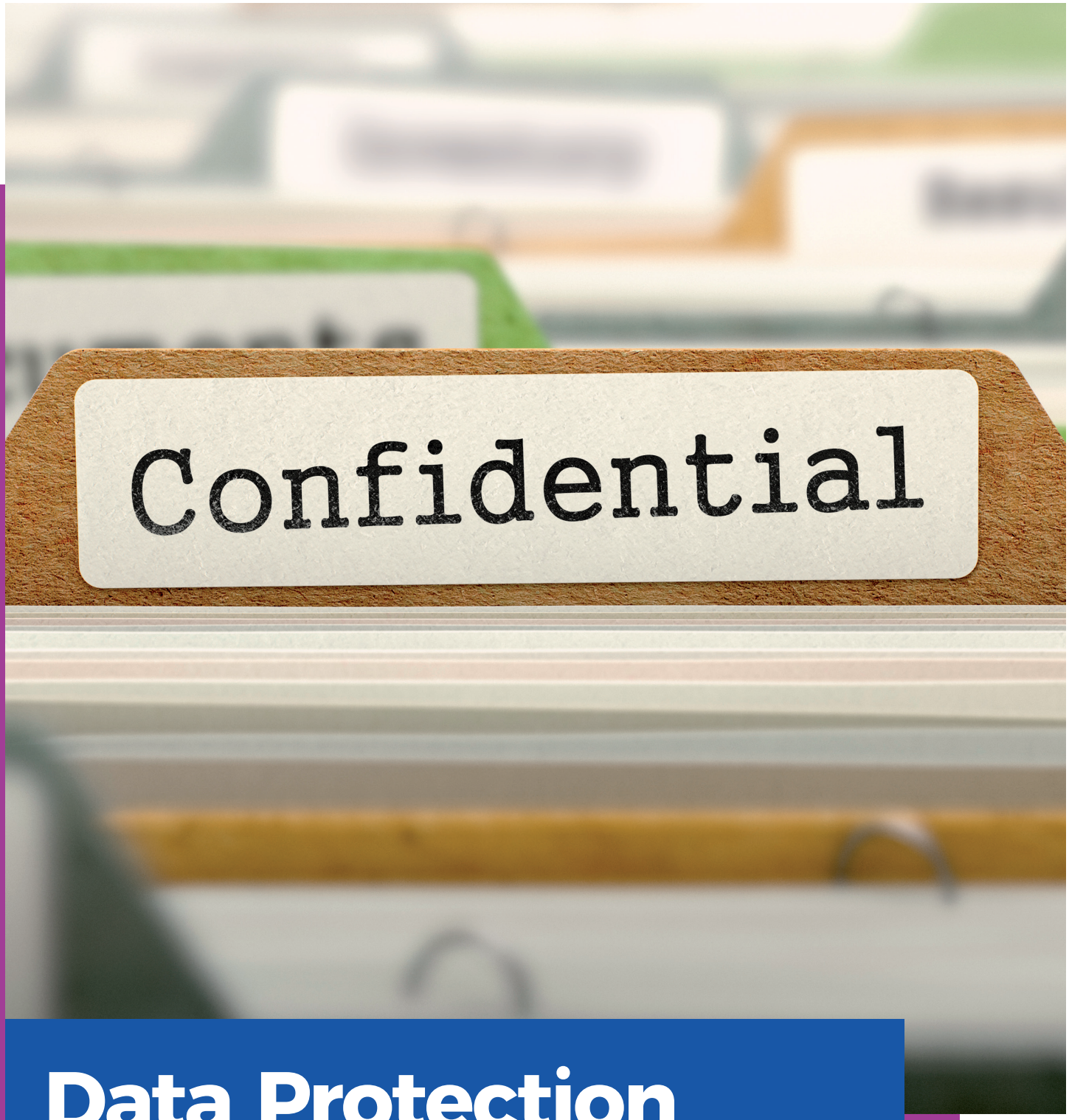

Data Protection

Compliance Training

EAST RIDING
OF YORKSHIRE COUNCIL

Contents

Welcome to your Data Protection workbook

About your workbook

Welcome to your training workbook on Data Protection. This training explains how to keep information safe in line with legislation (the law) and our own council policies.

All council employees must do some data protection training - this is known as a **data protection compliance indicator**. If you are not sure which training you should do please read the council's **Data Protection Training Procedure**, which is available on the intranet.

You can only use this booklet to achieve your **Data Protection compliance indicator** if you do not have council network (computer) access or have regular access to personal data as part of your job.

Using your workbook

This workbook contains lots of information about Data Protection and will use examples to help you understand what this is and how it applies to you.

Special language used to talk about Data Protection will be shown in **bold** and will be explained the first time you come across each one.

At the end of your learning, you'll need to speak to your manager so they can record that you've completed the training. You'll be able to keep your workbook so you can come back to it whenever you need to refresh your knowledge.

Section 1 - Introduction

Data protection legislation

The **United Kingdom General Data Protection Regulation** (UK GDPR) and **Data Protection Act 2018** (DPA18) are the current data protection laws in the UK. These are often referred to as **data protection legislation** or **laws**.

What is the purpose of the Data Protection Act?

The Data Protection Act 1998 was updated following a new European Union Regulation, the General Data Protection Regulation (EU GDPR). As the UK was part of the European Union (EU) at the time, GDPR became the law in the UKon the 25th May 2018.

The new Data Protection Act was needed to implement the **Crime Directive**, as this did not automatically apply in all EU countries. The Crime Directive was needed as it covered personal data to do with law enforcement, which GDPR did not include. EU 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.

Following the UK leaving the EU the EU GDPR was replaced by the UK GDPR on 1 January 2021. There is very little difference between the two laws.

Data Protection law reinforces common sense rules regarding information handling. They are there to make sure that we manage personal information in a sensible way and treat our customers and their information with respect.

Think about how you would want 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 large amount of personal data about each and every one of us! For example, you probably pay council tax, you may be a housing tenant, or 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. Not to mention sickness records, holiday records, training records, etc. - the list goes on.

Think about how you would you feel if your information or your family's information was not protected and was used in an irresponsible manner?

Role of the Information Commissioners Office

The **Information Commissioner's Office** (ICO) is a UK independent body. They uphold information rights for the benefit of the public and encourage openness by public bodies and also data privacy for individuals.

Businesses and organisations that handle personal data are required to pay a fee/register with the ICO as Data Controllers, unless they're exempt. The council is registered with the ICO.

Part of the role of the ICO is to take action to make sure that the council meets our information rights obligation. This includes monetary (financial) 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 (location and geographic information)
- Reuse of public sector information regulations.

Data protection headlines

Data Protection is often in the news; let's make sure the council stays out of the headlines!

Data protection key terms

The words used when talking about Data Protection can be confusing. The following is a list of the common words and phrases you may come across.

Consent

'Consent' means any freely given, specific, informed and unambiguous (clear) indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, shows agreement to the processing of personal data relating to him or her.

When people consent, they agree to something that they fully understand and have the right to say no to.

Data controller

'Data controller' can be a person (or an organisation) which decides the reasons and methods of processing personal data. The council is a Data Controller.

Data processor

'Data processor' is a separate individual or an organisation which processes personal data for the **Data controller**. An employee of the council is **not** a data processor.

Personal data

'Personal data' is any information about an individual which can identify them personally, such as a name, an identification number, location data, an online identifier or information about the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Data subject

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

Personal data breach

'Personal data breach' means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data; for example, leaving files about people in the back of a taxi.

Processing

'Processing' means work done with personal data, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction – basically anything that uses personal information.

Profiling

'Profiling' is the automated processing of personal data. This includes the use of personal data to assess certain information relating to an individual, such as to analyse or predict things like a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation

'Pseudonymisation' means amending personal data so that it can no longer be linked to an individual without the use of additional information. This extra information must be stored separately and technical and organisational measures must be taken to make sure that the personal data is not linked to an identifiable individual. An example of this might be referring to employees by their employee number, not their name.

Special category data

'Special Category Data' is personal data that reveals 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

This is personal data that is used for the purposes of prevention, detection, and prosecution of criminal offences or the execution of criminal penalties including safeguarding against threats to public security.

Supervisory authority

'Supervisory authority' means an **independent public authority** which is responsible for monitoring data protection. In the UK, the supervisory authority is the Information Commissioner's Office (ICO).

Section 2 – The principles of GDPR

Data protection principles

UK GDPR requires any organisations acting as either **data controllers** or **data processors** (see above section for a definition of these) to process data in line with the rules of data protection. There are 6 main principles with a 7th that requires you to show that you are meeting the 6 other principles.

Processed lawfully, fairly and in a transparent manner:

- When the data is collected, it must be clear why that data is being collected and how it will be used.
- The council must be willing to provide details about data processing when requested by the data subject (the person involved).
- For example, if the data subject asks who the **Data Protection Officer** is at the council or what data the council has about them, that information needs to be made available to them.

Purpose limitation:

- The council must have a lawful and legitimate purpose for processing the information in the first place.
- Think about all the information that the council needs in forms; for example, why have 20 questions in a form when you only really need a name, email and a phone number?
- Simply put, this principle says that the council shouldn't collect any data that is unnecessary, and if we do this we would not be following the law.

Data minimisation:

- The council must make sure that the data they collect is adequate, relevant and limited.
- In this day and age, businesses collect every piece of data possible for various reasons, such as understanding customer buying behaviors and patterns.
- Based on this principle, the council must ensure they are only collecting and keeping the minimum amount of data required for their purpose.

Accurate and up-to-date processing:

- Data Controllers should make sure that information is accurate, valid and fit for purpose.
- To comply with this principle, the council must have processes and policies in place to say how they will maintain the data they are processing and storing.

- It may seem like a lot of work, but an effort to maintain accurate customer and employee databases will help with compliance and hopefully also be useful to the business.

Limitation of storage in the form that permits identification:

- This principle limits how the data is stored and moved, as well as how long it is stored for, and requires an understanding of how a person could be identified if the data records were to be breached or accessed by someone who shouldn't have access to them.
- To ensure compliance, the council must have control over the storage and movement of data. This includes putting in place and sticking to **data retention policies** and not allowing data to be stored in multiple places. For example, the council should stop workers saving a copy of a customer list on their laptop or moving the data to another device, such as a USB stick. Having multiple copies of the same data in multiple locations is a compliance nightmare!

Confidential and secure:

- This principle protects the security and privacy of data by making sure it is secure (which includes both computer systems and paper records).
  The council is responsible for putting in place appropriate security measures that are in line with the risks and rights of individual data subjects (people). Negligence is not an excuse under GDPR, so the council must make sure that they protect data from those who are negligent or malicious.
- To achieve compliance, the council looks at how well they are enforcing security policies, controlling access, verifying the identity of those accessing the data and protecting against computer viruses.

Accountability and liability:

- This principle ensures that the council can show they are compliant. The council must be able to show the **governing bodies** that they have taken the necessary steps in line with the risk their data subjects face.
- For example, GDPR requires the council to respond to requests from data subjects regarding what data is available about them.
- The council must be able to promptly remove that data, if desired by the individual.
- The council not only needs to have a process in place to manage the request, but also needs to have a full audit trail to prove that they took the proper actions.

The principles are basically a code of good practice for processing personal data. Further information can be found at the Information Commissioner's Office website www.ico.org.uk.

Conditions for processing

Personal data must only be used (**processed**) if the council (**data controller**) has a lawful basis for doing so. If this does not apply then any processing will be unlawful and therefore in breach of data protection legislation.

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

Lawful basis

Personal data must only be processed under the following conditions:

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

As a council we should focus on public task, contracts and legal obligation

Special category data

Special category data can be processed under the following conditions:

- 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
- Public interest in the area of public health, scientific or historical research.

Law Enforcement Data

Law Enforcement data can be processed under the following conditions:

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

Fairness

In data protection, fairness means that the council should only handle personal data in ways that individuals would expect and not use it in ways that would have a negative effect on the individual. This links to **transparency** – being open and honest about how data is used. It would be unfair to mislead someone into providing their data by being unclear about your reasons for doing so.

Transparency

Transparency is about ensuring that the council is clear, open and honest about their intentions with individual's data, as well as who they are and why they are using the data. This principle links to the individuals' right to be informed, which you will learn about in Section 3.

Section 3 – Rights of the individual

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 be informed
An individual whose personal data is processed by the council will have the right to be informed about this. They will have the right to be informed about who, what, where and why the data is being processed.

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 information should be done in writing and ideally electronically.

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

The council makes every effort to make sure that 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 online at – www.eastriding.gov.uk/privacynotice

There is a list of things to include when providing privacy information to an individual whose data has been collected. They include:

- Name and contact details of the council.
- Contact details of the Data Protection Officer.
- The purposes that you are processing the information under.
- What information you are capturing.
- If you are sharing the information with others e.g. HMRC, NHS, DfE.
- The rights that individuals have.
- Explain that an individual can make a complaint.

Consent

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

- Opt-in
- Clear
- Affirmative
- Informed
- Freely given
- Unambiguous
- Auditable.

Consent must be a choice and people must be able to withdraw it. If consent is relied upon it also means that an individual's 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.

Right of access

Individuals are entitled to obtain access to their personal data on request, free of charge except in certain circumstances. These requests are sometimes referred to as **'Subject Access Requests'** (**SARs**).

An individual will be entitled to the following information:

- Confirmation that their personal data is or is not being processed
- Access to the personal data that is undergoing processing
- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular, recipients in third-party companies or international organisations
- Where possible, the expected period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The right to lodge a complaint with the ICO or any other relevant supervisory authority
- Where the personal data is not collected from an individual, any available information as to the source of that information.

Right to rectification

People can ask for their information to be rectified (corrected) if it is inaccurate or incomplete. Before any information is updated, we would need evidence from the individual.

The council has one month to respond to a request for rectification, any request should be sent immediately to data.protection@eastriding.gov.uk. Before any information is updated you should ask for confirmation and evidence of the proposed changes from the individual. If the information has been shared with another partner or organisation then the council will also need to inform them of the changes.

Right to erasure

The right to erasure can also be referred to as 'the right to be forgotten'. It means that individuals have the right to request that their data is removed from an organisation's database.

However, this is not a guaranteed right and is only valid in certain circumstances, such as:

- The data being no longer necessary for the original purpose it was collected or processed for.
- The data being reliant on the consent of the individual, which they are now withdrawing.
- The individual objects to the processing and there are no overriding legitimate grounds for the processing.
- The data is being processed for direct marketing purposes and the individual opposes this.
- The data has been processed unlawfully.
- The data has to be erased to comply with a legal obligation.

Any requests should be sent immediately to data.protection@eastriding.gov.uk.

When the right to erasure does not apply

The right to erasure does not apply if processing is necessary for one of the following reasons:

- To address freedom of expression and information e.g. a social worker's report of a child or incident that the parent may later contest, as it is their opinion.
- To comply with a legal obligation - you would not be able to delete Council Tax records of an individual who was currently living in the area as you have a legal obligation to hold, use and report on this information.
- For a task carried out in the public interest or in official authority - you could not delete resident's records from being held by the Refuse Collection team as the council has a public duty to provide everyone with a waste collection service.
- For archiving purposes in the public interest – such as scientific research, historical research or statistical purposes where erasure is likely to affect the outcome of that work.

- For the establishment, exercise or defence of legal claims. If there has been a serious accident within the council, you wouldn't delete any records in relation to this in case of later legal claims.

Right to restrict processing

Individuals are able to limit the way that an organisation uses their data, rather than simply having it erased. There is the right of restriction where an individual has a particular reason for wanting this restriction, e.g. they may have issues with the content of the information that is held about them or how their information has been processed.

Individuals have the right to restrict processing of personal data from organisations acting as data controllers in any of the following circumstances:

- The accuracy of the personal data is contested by the individual, so it is restricted for a period, so that the data controller can verify the accuracy of the personal data.
- There has been unlawful processing of information and the individual doesn't want their personal data to be erased and requests that it is restricted instead.
- The data controller no longer needs the personal data for the purposes of the processing, but it is required by an individual for the establishment, exercise or defense of legal claims.
- The individual has objected to the processing of their information (on the grounds of a public interest or legitimate interest) and is pending the verification of whether or not the legitimate grounds of the data controller outweigh those of the individual.

Where processing has been restricted, the personal data will (with the exception of being stored) only be processed with the individual's consent. It could also be used for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

Where an individual has successfully asked for their personal data to be restricted, the data controller will inform the individual before such a restriction is lifted.

In circumstances where the council is unable to comply with the request because it proves impossible or involves disproportionate effort, the council should document this.

Right to portability

Individuals have the right to receive any personal data about them that they have given to the council, which is held in an electronic format (in a common format, like a Word document) and have the right to transmit (copy) this data to another council or organisation where the processing is based on the individuals consent or a contract, and carried out by automated means.

This must be provided within one month, and be free of charge, however, the council is not required to have systems that are compatible with other organisations.

Right to object

An individual has the **right to object** to their personal data being processed or profiled for things to do with the public interest or any other legitimate interest.

Individuals have an absolute right to stop their data being used for direct marketing, scientific or historical research.

Continuing Processing

In other cases where the right to object applies, the council may be able to continue processing if they can show that they have an important reason for doing so.
If the council is confident that they do not have to comply with the request, they should inform the individual of this and also inform them of their right to complain to the **ICO**. For this reason it is important to document all decision making steps.

Rights related to automated decision-making, including profiling
An individual has the right not to have their data used in an automated decision-making process, including profiling, that produces a **legal effect** or a similarly **significant effect** on the person. The decision must have a serious negative impact on someone to be under this provision. This right only applies to automated decision making where there is no human involvement.

However, it is possible to subject an individual to automated decision-making processes, including profiling, where:

- It is necessary for entering into or performance of a contract with the individual.
- It is authorised by law.
- The individual has given their explicit consent.

An individual has the right to object to this sort of profiling and people can ask for:

- A human to be involved in the decision-making process
- The opportunity to challenge the decision
- An explanation of how the decision was made.

Section 4 – Data Protection Impact Assessments (DPIAs)

One of the ways the council makes sure people's rights are protected is by putting in **privacy by design**. The council is required to do this; this means that privacy should be at the first consideration in all decision making.

One of the ways we do this is by carrying out **Data Protection Impact Assessments** (DPIAs). We are required to carry these out by law for high-risk and large-scale processing. The DPIA process is a two-stage process, and the forms can be found on the Intranet.

DPIAs are considered best practice for any significant changes of the way we process personal information and one of the best ways of preventing issues and penalties later down the line.

The council has a process for carrying out DPIAs and anyone considering changes to the way in which data is used or collecting new data should contact data.protection@eastriding.gov.uk for more information.

Section 5 - Your role

Data breaches

'A data breach is a security incident in which information is accessed without authorisation. Data breaches can hurt businesses and consumers in a variety of ways. They are a costly expense that can damage lives and reputations and take time to repair.' - Norton Internet Security.

Responding to a data breach

If you suspect or discover that a data breach has occurred:

- It must be reported to the Information and Governance and Feedback team, without delay at data.protection@eastriding.gov.uk or Ext: 1419
- If it involved IT, it must also be reported to the IT Service Desk, Ext: 4444.
- For any incident relating to building security or misuse of a staff swipe badge it must be reported to Infrastructure and Facilities on Ext: 5990.
- The council is required to report certain data protection incidents within 72 hours. The 72 hours start from when a breach is discovered by an employee, so you must act quickly.
- Sometimes the council needs to inform those individuals whose data is involved or has been affected by the breach.

The process is not about getting staff into trouble, the focus is on the identifying the risks that may have led to the breach and looks at preventing breaches happening again, which helps to protect staff.

Some common examples:

- Leaving confidential papers/IT equipment in cars.
- Breaching policy - letting someone borrow your laptop.
- Not destroying confidential waste correctly.
- Security – letting someone to tailgate you (follow you) through the secure entrance at a council building.
- Sharing information that has been collected for one purpose but used for another.
- Ensuring emails are sent to the correct recipients.
- Inappropriate use of information – such as using council information for personal use.
- Mobile working – overheard conversations, screens being visible.

Dealing with SARs

All staff should be able to recognise a SAR and understand when people can ask for their personal information. Staff should be aware that a request can be both in written format and asked for verbally. People do not have to mention the correct legislation to request

information for it to be a valid request i.e. they do not have to state that they are making a Subject Access Request.

If you receive a request for information you must immediately pass it onto the Information Governance and Feedback team. Ideally you can send an email to data.protection@eastriding.gov.uk so that the team can deal with the request promptly.

How the council complies with SAR Requests

- All valid requests will be given a reference number and be logged. This will include the process of checking a the person's identity to make sure that they are entitled to receive the information they are requesting.
- Requests are free of charge and must be completed with 1 month (28 days). However complex requests can be extended by up to 2 months- this extension has to be approved and confirmed by the Information Governance and Feedback Team and only applies in very limited circumstances.
- Information may be provided to the requestor as a computer printout, letter, electronic files etc., but it must be provided in a way so that it can be easily understood with any codes or abbreviations explained.
- Where information is being provided to a child there may be instances where a member of staff would have to talk them through the information being received, or parts of it given to them using clear and plain language.
- Be aware of having to redact (block out) any third party information out of the information being requested. This is to protect other people's personal information e.g. if a noise complaint was made about the individual, the individual may not know who made the complaint, only the content of the actual complaint.

- Understand that there may be instances where the council doesn't release certain information if it may cause harm or distress.
- A **SAR** can be made on behalf of another person, e.g. via a parent/guardian or solicitor, but there must be the appropriate consent or authorisation in place to be able to do so e.g. power of attorney.

For further information about these requests please speak to the Information Governance and Feedback Team.

Redaction

What is redaction?

It is likely that as part of responding to a SAR (or other requests for information) that you may need to undertake some **redactions** on the information to be released. Just as individuals have a right to access, you also have to protect the information of third parties.

Redaction is the removal of sensitive 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.

Supplying un-redacted documents can have serious consequences for the individual. On the other hand, unnecessary redactions can result in people not getting the information they have a right to. Both can result in action from the Information Commissioner's Office (ICO).

Basic principles of redaction

- Always carry out redaction on a copy of the original record – not the original.
- Remove any third party information which should not be shared.
- You can contact the third parties and ask for their permission to release information if needed.
- If so much information has to be redacted that a document doesn't make sense, the document should not be shared at all.
- Redaction should be done or checked by staff that are familiar with the records.
- You should keep copies of what has been redacted and keep clear and thorough notes of the reasons why.
- You must make sure that no redacted information remains visible or is retrievable.
- Special redaction tools should be used.

Anonymisation

Involves amending the data either by removing any obvious personal identifiers or by summarising data.

This might include:

- Removing names and addresses, etc.
- Replacing date of birth with an age band e.g. aged 18-24
- Reducing length of time to a time band e.g. <2 years, >5years
- Providing only a partial postcode
- Removing data that are not relevant to the analysis to be undertaken
- For record level data.

Pseudonymisation

Attaches a coded reference (pseudonym) to each record so that they can be linked with a particular individual without that individual being identified, like in the example of employee numbers used earlier.

Requests about other people

Where a Subject Access Request is made about a child, the information would only be released to a person with parental responsibility, and the best interests 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.

In some circumstances 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 still need to be logged and a record kept of what is released, to who and why. Again these requests should be forwarded to the Information Governance and Feedback Team at data.protection@eastriding.gov.uk.

Accountability

As explored in Section 2, **accountability** is one of the key principles of UK GDPR. It makes both individual people and organisations responsible for complying with data protection legislation.

To comply with this principle, the council has put in place both technical and organisational measures, which all employees must stick to.

Examples of compliance measures that are in place include:

- Adoption of a Data Protection Policy
- The appointment of a Data Protection Officer
- Maintaining Records of Processing Activity (ROPA) i.e. details of all personal data that the council holds). This is split up by each individual service area
- Recording and reporting personal data breaches
- Having appropriate privacy notices in place
- Undertaking Data Protection Impact Assessments where required.

Records of Processing Activity (ROPA)

The council is required to hold **detailed records** of their data processing. The records must show the following information, which will be used by the **ICO** to hold us to account.

Any organisation that processes personal data needs to make sure they have records of what they process, including:

- 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).

Your work should be reflected on this document.

Information sharing

In order to share information between the council and another organisation there should be an **Information Sharing Agreement** (ISA) in place. This ensures that it is clear what information is going to be shared, why it is being shared and what safeguards are in place to ensure that information is securely shared. If required, the council will also seek an individual's consent around sharing information with third parties.

Additionally, you should not be sharing any information **verbally** if you do not have the authority to do so. This includes any information that may have been overheard as a result of sharing office space, as information discussed within the council may have safeguarding risks or commercial (business) consequences and can lead to the reputation of the council being damaged, if information is shared inappropriately.

If you are planning to share information with other organisations, for example other councils, you must be confident that we are allowed to share the information and be able to justify why the sharing is lawful if asked. If you are ever unsure please speak to the **Information Governance and Feedback Team**.

Data transfers

Remember that transfers of personal data to other countries is controlled by data protection legislation. If anyone wants to transfer data outside of the UK they need to ensure they have a lawful reason to do so. Further guidance can be sought from the Information Governance and Feedback team.

Consequences of failing to comply

Failing to comply with UK GDPR can have serious consequences for an organisation. The maximum fine is up to 4% of annual global turnover or £18m, whichever is greater for organisations that breach the requirements.

Reputational Consequences

Alongside any financial penalties the council's reputation can also be damaged as result of failures to comply with data protection. This can include unwanted media attention, bad publicity, and losing residents' trust.

The **Information Commissioner's Office** (ICO) has fined a London-based pharmacy £275,000 for failing to ensure the security of special category data.

Doorstep Dispensaree Ltd, which supplies medicines to customers and care homes, left around 500,000 documents in unlocked containers at the back of its premises in Edgware. The documents included names, addresses, dates of birth, NHS numbers, medical information and prescriptions belonging to an unknown number of people.

Section 6 – Summary

Why does data protection matter?

Data protection matters because we must follow the laws about how personal information is used, this includes making sure it is 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
- Report when our policy has not been followed
- Keep confidential information secure
- Not carry out illegal, libellous, immoral or offensive activities
- Use your council access and identity only in a way that is in line with your role
- Follow their rules when using another organisation's network (computer system)
- Make sure that other people follow the council policy if you are a manager.

What happens to information?

- We ensure that information is processed in line with the **7 data protection principles**. These act as a basic checklist for how you use personal information
- Information that we hold is stored and accessed for business reasons
- After statutory (lawful) and recommended minimum retention periods, information is destroyed and disposed of correctly
- You only share information if you are confident you are allowed to share it.

Protecting information

- Data protection is all about risk management
- Always report breaches so risks can be identified
- The **Information Governance and Feedback** team are here to help, if you are unsure, please ask.

Refreshing your training

In line with council policy you will be required to refresh 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 you can contact your Information Governance and Feedback Team (ext: 1419) or email data.protection@eastriding.gov.uk.

For more information look at the ICO web site www.ico.gov.uk.

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