Keeping personal information safe

Bolton Council

GDPR Summary

- **GDPR** is a new data protection law which came into effect from 25th May 2018
- People have the right to request information we hold about them
- All use of information must be lawful and you should tell people what you are doing with their information
- Privacy terms for any organisation who want to share or communicate with their customers have changed
- Individuals have more rights over their personal data
- Organisations are required to ensure GDPR compliance
- A Data Protection Officer will be tasked with queries relating to data protection, to help keep the organisation compliant and to report issues to the governing body where necessary

What is Personal Data?

Personal data is information we hold that relates to an **'identifiable living individual'**
This means any detail in any format (including photographs) that can be used on its own, or alongside other data, to identify them
Note: It can be the expression of an opinion about the individual

You wouldn't want just anyone sharing your child's photo on Facebook

We must justify why we use people's information and sometimes we may ask people for their consent.
You may have been asked by companies if you still want to hear from them. We have done the same for people who want to hear about what we do.

Collecting Personal Data

- When we collect information from people we should explain what we will be using it for, why and how long we will keep it
- Collect only the data you need for the purpose of the role. Do not record excessive information
- Information must be accurate and kept up to date
- We must only keep the information for as long as we need it
- The information must be held and processed securely
- Personal data must be processed lawfully which means that:
  - The person has given consent or
  - We need the info to perform a contract or
  - We need to legally hold the information or
  - We need to protect the person or
  - We need to carry out a task in the public interest

If you are currently handling personal data correctly, the GDPR will probably not make much difference to your day to day working.

People's rights

GDPR means that individuals have the following rights:

- the right to be informed about how their information is being used and stored;
- the right to find out what information we hold about them;
- the right to amend any mistakes;
- the right to ask for information to be erased;
- the right to restrict processing;
- the right to ask for information to be moved to another provider (data portability);
- the right to object to the processing of information about them; and
- the right to object to automated decision-making

There are exemptions to these rights and we will have the right to refuse in certain circumstances.

Special Category Data is Sensitive Data

Race, Ethnic Origin, Political Beliefs, Religious Beliefs, Trade Union Membership, Genetics, Biometrics (where used for ID purposes), Health, Sexual Orientation

Examples of Personal Data

Name, Age, Address, DOB, Email Addresses, Telephone Numbers, Medical and Financial Records, Sickness Records, Annual Leave, Training Records, Pension Details, Descriptive Information, Notes on Systems, Call Recordings, Minutes of Meetings

Information Security Breach - Examples

A breach is when personal data has been lost, misplaced, accessed unlawfully, shared with the wrong person, altered or destroyed either accidentally or wilfully

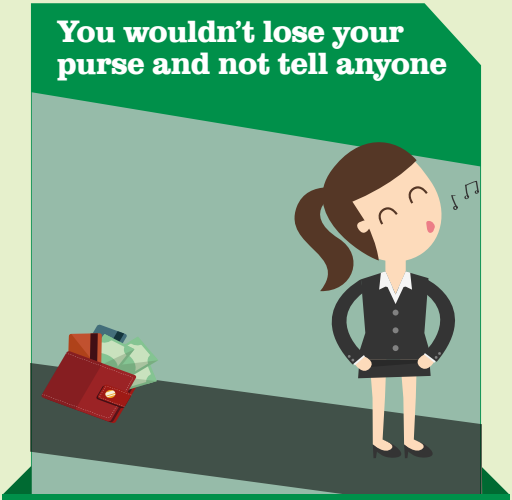
e.g. Accessing unauthorised data, misdirected email, loss of paperwork, stolen or lost laptop, lost memory stick, giving personal data out to an unauthorised person, posting a letter to the wrong person, leaving data in public view e.g. desk, cars

Reporting a Breach

- Contact your manager
- Your manager will report the incident to the 'Information Governance' (IG) team – they support services across the council
- A breach of security is a disciplinary and potentially a criminal offence
- Each incident is investigated (lessons learned)
- Don't waste time! You must always report a breach within 24 hours
- The consequences for the council and any individual person responsible for a breach can be worse if left unreported

Request for Information

- People have the right to request information we hold about them in whatever format we hold it. This is called a **Subject Access Request.**
- The '**Information Governance' team (IG)** are the central point for the request, information.security@bolton.gov.uk
- **Subject Access** requests are now free of charge and we have 1 calendar month to process. If it is complicated this time may be extended.
- Subject Access requests are not to be confused with Freedom of information request (FOI), they need to be sent to the freedomofinfo@bolton.gov.uk



Despite everything we do sometimes things can go wrong. If you believe that someone's personal information has been leaked – called a breach – you must report it. Failure to report a breach could result in the council facing fines.

Examples of Data Requested

Information held in system/databases, HR records, meeting minutes, tape recordings, CCTV images, photographs, emails, paper records (post it notes, diaries, case files)

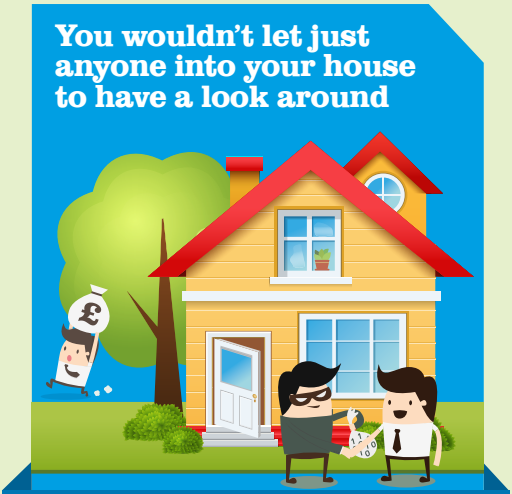
Request for Information - Third Party Request

What are they?

Request for someone's personal data which is not their own. e.g. Police, HMRC, other councils, Insurance companies.

What to do

- DO NOT give information over the phone or in person
- Ask the requestor to complete our third-party form (available from: information.security@bolton.gov.uk)
- If in doubt, don't give it out and check with the IG Team



People have the right to ask for the personal information we hold about them.
But we wouldn't give out the information without doing some checks.
Asking for information is called a 'Subject Access Request'.

We need to make sure that if we must share personal information that we do it properly.

Minimise Risk

Paper

- Don't leave personal data notes unattended
- Check photocopiers before you walk away
- Don't leave personal data in public view e.g. desks, cars
- Face to face, remember to clear away other people's data before you deal with a new person
- Keep personal data in locked cabinets
- Dispose of via cross cut shredder, confidential waste bins/bags

Verbal Communication

- Be aware when holding meetings in public spaces
- Could colleagues sharing the workspace see or hear, or customers in the coffee shop or pub hear you using/sharing someone else's personal data?
- Would you want people to meet and discuss you and your personal information in public or private?

Equipment/Systems

- Only use approved ICT equipment
- Do not store any information to the PC or phone
- Do not use memory sticks to transport personal data
- Lock PC's, tablets before you leave your desk
- Don't share passwords
- Don't access systems or information not relevant to your role

Post

- Where possible send sensitive information by secure email (Egress) instead of posting or hand deliver it
- In the event that there is no alternative, sensitive personal data that is sent out by post must be double enveloped, sealed, marked 'Confidential' on the outer envelope, sent recorded/tracked and include a return address e.g. care assessments on the inner envelope
- Internal post containing Sensitive Information must also be in a sealed envelope, marked private and confidential and include a return address e.g. social care assessments

Email/Skype Communications

- Never send or receive work via personal email addresses, they aren't secure
- Do not include personal details in the subject heading
- Always check the recipients are correct before pressing send for both internal and external emails
- Think about the content, don't include derogatory remarks or comments about staff or the public in emails, they are subject to disclosure as part of a Subject Access Request
- Skype communication are also subject to disclosure

You wouldn't let other people see your bank details

We need to make sure that we keep any sensitive, confidential and personal information about people safe. Any place - printed information, memory sticks, CDs, computers – where we hold personal information about people needs to be protected. Losing the information on them could be costly for them and us.

I have read and understood this guidance notes about GDPR

Employee Pay No.	
Name (Print):	
Department:	
Date:	
Signature:	

HR Privacy Notice

As well as collection personal data about members of the public the council also holds information about you as council employees. The HR Privacy Notice is available on our intranet. **bit.ly/2uHKGOe**

It describes how we collect, use and share personal information about you:

- before, during and after your working relationship with us, and
- the types of personal information we need to process, including information the law describes as 'special' because of its sensitivity.

If you don't have access to the internet, please ask your manager for a copy of the HR Privacy Notice.

Bolton Council