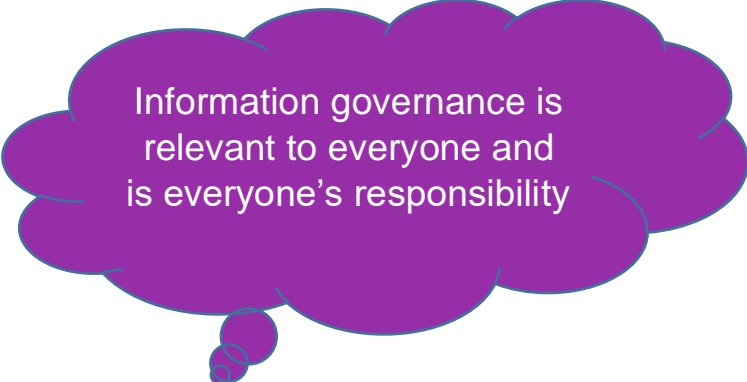


# Understanding Information Governance Course

## About this Document



Information governance is relevant to everyone and is everyone's responsibility

This training document has been provided to you as you have been identified as not having access to a laptop or computer as part of your role. If you do have access to a laptop or computer as part of your role, you should complete the online Information Governance e-learning module:-

Every employee should have an understanding of Information Governance and have read the Council's guidance available at [www.staff.derbyshire.gov.uk/information-security](http://www.staff.derbyshire.gov.uk/information-security) If you are unable to access this website speak to your manager and they will arrange for hard copies of the relevant guidance to be made available to you. The Council takes its responsibility for information governance, data protection, information security and confidentiality very seriously. Any issues in these areas can lead to vulnerability for the individuals concerned, a loss of trust in the Council, as well as large fines being imposed which is money far better spent on providing services.



## What is 'Information Governance' and

### 'UK GDPR'?



Information Governance is the framework which enables the Council and you as an employee, to comply with legal and statutory requirements (mainly under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA)).



## The law on Data Protection

The UK GDPR and DPA enhance individual's rights over their personal data and strengthen the rules around how organisations use it.

For more information see [www.derbyshire.gov.uk/gdpr](http://www.derbyshire.gov.uk/gdpr)



## How the Council Manages its Data and Information

The Council is responsible for the safe handling of large amounts of personal data. This means that there must be a common approach followed by *all* staff. In order to comply with the legislation, the Council has developed a number of policies and procedures relating to keeping data safe and processing it lawfully. Copies of policies and procedures are available on the Council's website.



## Keeping Information Secure



We all use information on a daily basis and most of us will come into contact with other people's data at some point during the day; this could be just someone's name and address or more sensitive information, such as details of someone's disability.

Securing our computers, mobile devices and phones is now second nature but do not forget that paper records should be kept equally secure. The scrap of paper that you just wrote a name and telephone number on must be kept safe too. It should also be disposed of securely ~ throwing it in the nearest bin is just not good enough! This also applies when individuals are working at home too. Please ensure that any confidential documents requiring destruction are disposed of securely at a Derbyshire

County Council establishment.

It is equally important to be careful what we say too:

- **Always** be aware of who you are talking to, what you are saying and who may be able to overhear.
- **Never talk** about confidential work matters with friends, family, other service users or colleagues unless the colleague needs to know to do their job.
- **Be aware smart** devices and applications such as Alexa, Siri and Echo Dot may be "listening in" when they are close to you. If you are discussing work related matters unplug or mute smart speakers/ microphones, or ensure that they are out of earshot.
- **Don't be tempted** to use your personal email accounts to forward on personal data for work purposes. The Council's email system is secure and should be used for the transmission of personal data.
- **Always ensure** you know the identity of someone before passing information to them and only when it is appropriate and safe to do so. **If in doubt ~ DO NOT disclose the information!**

To help us, all documents (paper or electronic) should be classified as one of three types:

**Restricted** – information which, if disclosed (even within the authority) would cause serious damage in terms of financial loss, legal action or loss of reputation.

**Controlled** – information that is generally available to anyone in certain areas of the authority and which contains business value to the organisation or requires protection due to personal data.

**Public** – information that can be made freely available in the public domain and would not cause damage or harm if released.

Council badges must always be clearly worn so that others can satisfy themselves that we are who we say we are and likewise employees should ask for proof of identification from anyone they do not know or recognise.

## Reporting Security Incidents

**If you become aware of a security or confidentiality problem, or if an incident has occurred, you must immediately report it to your line manager or the service desk by calling 01629 537777**

Incidents include:

- Loss of Council ID badge.
- Loss, theft or disclosure of confidential or sensitive data or emails.
- Loss, theft or disclosure of confidential or sensitive written data or photocopies.
- Receipt of suspicious emails asking you to click on links or disclose personal information or virus warnings alerts appearing on a work device.
- Loss or theft of equipment such as, mobile phones, laptops, USBs, DVDs or external hard drives.
- Finding sensitive or confidential information.

Also if you become aware of something that you think could be a potential risk to security or confidentiality, you should consider whether to report it via Service Desk Online or by phoning the service desk on 01629 537777. If you are unsure about whether or not to report an incident, you can obtain guidance from your line manager or supervisor.

Potential risks include:

- Doors propped open.
- Delivery vans unattended with doors open.
- Screens sited near windows or where they can be overlooked.
- CCTV cameras not working.
- Documents left in printers, scanners or fax machines.



## What is Personal and Special Category Data?

All employees are expected to be able to recognise personal or special category data and know what to do to keep it secure. Special category data is subject to more stringent controls and needs to be treated with extra care. This is relevant to everyone, whether working at a desk/computer, out in the field or at the frontline of service delivery. The following brief lists will help you better understand what is classed as 'personal data' and what is classed as 'special category data':

Personal Data	Special Category Data/ data requiring additional protection*
<ul style="list-style-type: none"> <li>• Name</li> <li>• Date of Birth</li> <li>• Gender</li> <li>• Details of Current Address</li> <li>• Details of Previous Address</li> <li>• Family Relationships</li> <li>•</li> <li>• Telephone Numbers</li> <li>• Identity Numbers e.g. NI number or NHS number</li> <li>• Anything which enables us to identify a person</li> </ul>	<ul style="list-style-type: none"> <li>• Racial or Ethnic origins</li> <li>• Religious Beliefs</li> <li>• Sexual Orientation</li> <li>• Physical or Mental Health</li> <li>• Political Opinions</li> <li>• Trade Union Membership</li> <li>• Criminal Records*</li> </ul> <p><b>NB any documents containing special category data should be marked as 'Restricted'. Criminal records are highlighted as they are too very sensitive. They are governed by a different law but this often works in a similar way to the UK GDPR.</b></p>

UK GDPR now places an even greater importance on *all of us* to manage personal data securely and use it appropriately.

## Individual Rights

UK GDPR gives individuals a number of rights, the most common being the right to access the information the Council holds on them. The Council collects information about lots of people and for lots of reasons, from employees, volunteers and user users.

To find out more information about what the Council holds and what we do with it, please look at the [Council's Privacy Notices](http://www.derbyshire.gov.uk/privacynotices) online at [www.derbyshire.gov.uk/privacynotices](http://www.derbyshire.gov.uk/privacynotices) or ask your manager for a copy.

It is important to remember, if someone asks you for a copy of their information that you must pass it to your line manager or the Access to Information Officer (details below) immediately, as the Council has a strict time limit to respond.

## Freedom of Information (FOI) and Environmental Information Regulations (EIR)

The Freedom of Information Act 2000 and Environmental Information Regulations 2004 provide public access to information held by public authorities. Members of the public are entitled to request information from public authorities and public authorities are obliged to publish certain information about their activities.

Employees, may be approached to provide information under FOI or EIR. If this happens, the employee should make a note of the person's question and contact details and pass this on to their manager.

The member of public should also be provided with details of who to contact to deal with their enquiry further. These are as follows:

The Access to Information Officer  
County Hall  
Matlock  
Derbyshire DE4 3AG

Email: [access2info@derbyshire.gov.uk](mailto:access2info@derbyshire.gov.uk)



**The Council must respond promptly and within 20 working days.**

## Safeguarding and the Data Protection Act



Data Protection legislation is not a barrier to sharing information. Sometimes it is necessary to share information quickly to prevent death or serious harm. If you are asked to share information for safeguarding reasons, then you should immediately contact your line manager or a member of the Council's information governance team to discuss how this matter should be progressed.

## An Information Governance Check List for You

- ✓ Always wear your ID badge. If you are in a role where it can't be worn, ensure you have it to hand if challenged.
- ✓ Read and understand this booklet.
- ✓ Adhere to all policies and procedures you have been asked to follow.
- ✓ Do not use personal mobile phones or computers to share confidential data via text, email or social media.
- ✓ Never use social media (Facebook, Twitter etc.) to discuss work business.
- ✓ Do not leave paperwork lying around, lock it away or dispose of it securely.
- ✓ Ensure that you are not overheard when discussing personal data on the phone or with colleagues.
- ✓ Always verify a recipient's identity and authorisation before sharing personal data with them, particularly where telephone contact is involved.

- ✓ Read and comply with the Information and Communication Technology (ICT) Acceptable Use & Password policies
- ✓ Use strong passwords to access software applications. Include Upper case and lower case letters, numbers and special characters e.g. \* £ \$
- ✓ Never share or write down passwords.
- ✓ Always lock electronic devices that store personal data when not in use.
- ✓ Do not divulge door codes or allow 'tailgaters' to follow through behind you.



**Want to Know More?** Further guidance can be found on the Council's website, accessible from any computer; at <https://staff.derbyshire.gov.uk/information-security/information-security.aspx> and [www.derbyshire.gov.uk/gdpr](http://www.derbyshire.gov.uk/gdpr)