Nottinghamshire County Council

Be Data Wise

Their information. Your responsibility.

Be Data Wise

We all expect data about our personal lives to remain private and confidential.

At Nottinghamshire County Council, we come into contact with people's personal data at all sorts of times. From names and addresses, email and bank details to important social care information about people's backgrounds and medical history.

Protecting confidential information is everyone's responsibility. Take steps to make sure you know what to do.

This guide explains how to keep personal and sensitive information private and confidential.

The Data Protection Act 2018 (DPA)

The Act contains 6 six principles you must follow when handling personal data.

Personal data must be:

1. processed lawfully, fairly and in a transparent manner
2. collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes
3. adequate, relevant and not excessive
4. accurate and up-to-date
5. held no longer than is necessary
6. processed securely using appropriate technical or organisational measures.

What are personal data?

Personal data are any information that can potentially identify an individual.

They can include:

- name
- date of birth
- gender
- identification number
- physical data (e.g. photo)
- location data (address)
- online identifier (e.g. an IP address).

What are special category data?

These are personal data that are considered particularly sensitive and merit specific protection:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data (e.g. saliva, blood or urine results)
- biometric data (e.g. facial images or dactyloscopic data)
- health
- sex life or sexual orientation.

Access to Records Requests

The Data Protection Act also says that the 'data subject' – the person who the record relates to – can request a copy of their records.

The Complaints and Information team deals with these requests. Contact **accesstorecords@nottscc.gov.uk**

The Freedom of Information Act (FOI)

The Freedom Of Information Act (FOI) 2000 gives anybody, anywhere in the world, the right to know about any recorded public authority information, subject to exemptions, that is printed, written, taped, e-mailed, videoed or photographed.

All requests made under FOI must be made in writing, provide a name and address for correspondence and describe the information that is wanted. Requests can be written in any medium for example e-mail, letter fax, etc.

The Council must respond to FOI requests within 20 days.

These are dealt with by the Complaints and Information team. Contact **foi@nottscc.gov.uk**

How do I report a data loss?

Act immediately! It might be possible to retrieve the data or take steps to minimise any problems caused by the loss.

- If you lose confidential paper files, always inform your line manager. They should inform the Complaints and Information team as soon as possible. Email **complaints@nottscc.gov.uk** or call **0115 977 3788**.
- If you lose ICT equipment or your mobile phone, inform your line manager and ask them to contact Vodafone on **03333 0433333** to disable the device. Remember to also inform the ICT Service Desk on **0115 977 2010**.

How to be Data Wise

Follow these steps and you'll be well on the way to being Data Wise!

- Lock it when you leave it! Always lock your PC or tablet device when you're away from your desk.
- Always wear your ID badge.
- Keep up to date with best practice by completing your data protection and information management training.
- Before sharing information over the phone, always ask for a call back to make sure you are talking to the right person.
- Keep confidential social care cases private – use meeting rooms not the open plan office or corridors for discussions.
- Shred all confidential information or use the blue confidential waste bins.
- If you use a Word template to create files, delete all the existing information, or better still, use an original blank copy.

Safeguard your data

Using a PC

- Never save sensitive information to your desktop or computer's hard drive.
- Always save documents to the shared drive for your service area to make sure other people can retrieve them in our absence.
- Lock your computer when you leave your desk to prevent anyone accessing your files.
- Never download anything from the web – it could harm your computer or mobile device.
- Do not open suspicious emails with an attachment – it could be a virus.
- Always log off and shut down your computer at the end of the day.

Safeguard your data

Using email

- Make sure you are sending the email to the right person. Double check the spelling and don't rely on autofill for the email address.
- On group emails, use 'bcc' to make sure all recipients don't receive everyone else's addresses. Be careful when using the 'reply all' button - does everyone need the information?
- Send emails containing sensitive information or attachments using Cryptshare. The recipient doesn't need Cryptshare installed on their device to open and read the email.
- Do not forward emails containing confidential documents.

Safeguard your data

Sending post securely

If you are posting sensitive personal information like social care records, complaint investigation reports and safeguarding meeting minutes consider alternative postal delivery methods including:

- **Recorded or Special Delivery** may be used in order to track documents containing sensitive personal information to their intended destination and to ensure we have a record of delivery.
- **Courier or Special Delivery** may be used in order to ensure documents are delivered to their intended recipient by a certain time, for instance, to comply with a Court deadline.
- **Consider** organising face-to-face meetings with families to discuss written reports – it reduces the risk of files getting lost or delivered to the wrong address.

Before posting sensitive information:

- Keep address lists up-to-date in systems and databases to minimise sending information to the wrong person.
- Confirm the name and postal address of the recipient.
- Use a strong, **sealed** envelope for internal and external post.
- Make sure that the name and address of the recipient is clearly marked on the envelope.
- Always mark sensitive information **'Private and Confidential. To be opened by addressee only'** and ensure this is visible on the envelope.
- Always use the Council Letterhead template when sending sensitive information.
- Delete draft copies of documents – keep only one up-to-date version of your files and correspondence.
- If using a courier bag ensure that the courier bag is addressed to a named recipient.
- If the courier bag contains information for multiple addressees ensure that all information contained within the courier bag is in sealed addressed envelopes.

Safeguard your data

Security passwords

- Do not share your network log-on password with anyone – not even your line manager.
- Never write your password down. It must remain private and known only to you.
- Use a secure password – at least ten characters in length with a combination of numbers, letters, symbols and upper or lowercase letters.

Safeguard your data

Laptops, USB and DVDs

- Only use an ICT approved mobile device with the latest security and encryption features.
- Do not leave your mobile device unattended in a public place.
- Think about where you work – make sure nobody can see confidential files and data.
- Do not try to use your own USB stick – only ICT approved ones are compatible with our systems and contain encryption coding to keep them secure.

Safeguard your data

Printing and photocopying

- Never leave confidential papers on a photocopier.
- When you collect your printing, check you haven't picked up someone else's papers by accident.
- Always use the confidential waste bins to dispose of sensitive information. Or shred documents if no bins are available.
- Don't keep confidential files at home or in the car. They could be stolen or get picked up by other people. Keep paper files securely locked in the office.
- Always proof read reports and case files – make sure the individuals listed are the people you are meant to be writing about.

Safeguard your data

Taking photographs and video

- Do not use your own mobile phone to take or store photographs in case the device is lost and the data is found and used by someone else.
- Never take pictures or video without consent from the individual or their representative.
- Images required for safeguarding purposes do not need permission and should be kept with the appropriate case record. Store photos and images securely using the Total Mobile system. Delete any photos from a mobile device within one working day.
- Photographs and videos for the media require a consent form to be completed.

Safeguard your data

Home and mobile working

- Always lock your tablet device when you leave it unattended.
- Access your work files and emails securely using the ICT approved Get Connected system.
- When you are on the move, do not leave your mobile devices visible in your car or at home. Keep them secure to avoid theft.
- Do not send sensitive work emails to your personal home email address as this may not be secure.
- During face to-to-face visits, only carry the information you need – don't bring along case notes for other meetings.
- If you lose ICT equipment, make sure you report it immediately.

Safeguard your data

Phone calls and conversations

- When you make a call and discuss confidential information, think about where you make it. Who else can hear you?
- Always put calls on hold so that the caller cannot hear any other conversations in the office.
- Do not discuss confidential work matters with friends, family or colleagues.

Safeguard your data

Faxing

- Double check fax numbers before you send.
- Phone or email after sending the fax to check it has been received.
- Always use a cover sheet for your fax stating who it is for.

Safeguard your data

Office security

- Do not leave sensitive information lying around for anyone to read.
- Always follow the clear desk policy and lock your paperwork in your storage locker.
- Always wear your ID badge to make it easy to spot unauthorised people in the workplace.
- Inform reception if you are expecting any visitors and always sign them in and out of the building.
- Don't keep information for longer that it's needed – all teams should keep retention schedules under review.

Safeguard your data

Disposal of files and equipment

- Use the confidential waste bins to dispose of any paper waste.
- Do not throw away sensitive files or ICT equipment like USBs and mobile devices at home. It should always be securely disposed of at work.

Further information

To find out more about data protection please contact:

The Complaints and Information Governance team

Email: **complaints@nottscc.gov.uk**

Tel: **0115 977 3788.**

Further information is available on the intranet at:
nottscc.gov.uk/bedatawise

The IT Security Policy
nottscc.gov.uk/itsecurity

Data Protection
nottscc.gov.uk/dpa

Be Data Wise

Their information. Your responsibility.

Nottinghamshire County Council

W nottscc.gov.uk/bedatawise
E complaints@nottscc.gov.uk
T 0115 977 3788

facebook.com/nottinghamshire

@NottsCC

D&P/16-07/PP&CS/7927