Data Protection
and
Information Security

A WORKBOOK to help you work safely with personal and confidential information

Contents

About this workbook

Who it's for…

This workbook is for Norfolk County Council employees (including part time employees and retained firefighters) and volunteers who do not have access to the Council's computer network but handle or have access to personal information in these roles.

Norfolk County Council is required by law to make sure you are aware of our organisation's procedures for handling personal information.

The purpose of this workbook

This workbook aims to:

1) Explain why Norfolk County Council places such importance on data protection and information security

2) Help you understand how the General Data Protection Regulation (GDPR) applies to you and your responsibilities

3) Highlight the policies, procedures and best practice that Norfolk County Council expects you to follow when handling personal and confidential information

How to use this workbook

Your manager will talk with you about how to use the workbook and any other guidance you need in this topic.

By the end of the training you will have:

- Learned about how to handle data protection and information security in your role
- Completed the quiz at the end of the workbook and discussed your answers with your manager
- Signed the statement at the end of the workbook to confirm you understand fully your role and responsibilities in data protection and information security at Norfolk County Council

The GDPR

The GDPR came into force on 25th May 2018 and replaced the Data Protection Act 1998. It requires us to ensure that all personal information collected and used is kept secure and handled in accordance with the GDPR.

Why it's important for Norfolk County Council and for you

We handle huge amounts of personal information about members of the public and employees including service delivery and financial data.

Most of this information is collected, used and stored on computers and transmitted across networks to other computers. But we also transmit and receive personal information in, for example, letters, verbal reports and telephone calls and record personal information on paper records.

Each of us has a responsibility to make sure we deal with this information properly, no matter how it is collected, recorded and used – whether on paper, in a computer or in other ways.

The consequences of a breach of the GDPR

If we do not handle this information in accordance with the GDPR, we could cause substantial distress or damage to people – service users, customers, members of the public or colleagues. For example, a data protection breach could lead to fraud and identity theft.

Breaches of the GDPR can also result in damage to the council's reputation and potentially huge fines by the Information Commissioner (**up to £17.6 million, or 4% of our total annual turnover, whichever is higher)**

These are real examples of fines and breaches relating to Norfolk County Council ….

- paper records found in a skip
- paper records found in a filing cabinet purchased second-hand by a member of the public
- personal information faxed to the wrong address

We were fined £80,000 in February 2012 for delivering a confidential report to the wrong address.

Also, under the Data Protection Act 2018, staff and volunteers will be committing a criminal offence if they "knowingly or recklessly" access personal information they don't have a right to see, or disclose or retain personal information without the authority of the County Council

What is ‘personal information’?

Personal information is information relating to natural (living) persons who:

- can be identified directly from the information, or
- can be indirectly identified from that information in combination with other information.

Some examples of personal data…

- Name
- Age
- Marital status
- Postal address
- Email address
- Telephone numbers
- Location data
- Bank details
- National Insurance Number
- Vehicle number plate
- Medical records
- Disability
- Religious belief
- A criminal conviction
- Photograph
- CCTV images
- Online identifiers like IP addresses and cookie identifiers
- …and even an opinion about an individual

The six key data protection principles

The GDPR sets out six data protection principles which form the backbone of the GDPR. We have a duty to comply with these principles and that failure to comply will breach the GDPR which may lead to a fine.

Some of these principles will be directly relevant to what you do. Others less so. But it is useful to be aware of all of them.

1. **Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals**

   If we are collecting personal data we must tell that person what personal data we need to collect about them in order to provide our service, why we are collecting it, who we collect it from and who we share it with. We also have to tell them their rights under the GDPR

   Example…
   When someone joins a library, we must tell that person what personal data we need to collect about them in order to be able to lend books, DVDs and CDs to them (e.g. their name and address). If we then want to use their information in a different way, we must inform them.

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

   If you collect or use personal data for one **purpose**, you can't suddenly decide to use it for something completely different

   Example…
   If the Fire Service collects personal information from fire risk check of homes, we cannot give that information to the museum service to enable them to write to that person about their membership schemes.

3. **Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are used**

   We must only collect the minimum amount of personal data we need to fulfil our purpose. We can hold that much information, but no more.

   Example…
   If we are never going to telephone an individual, we should not ask for their telephone number.
   If we only need to know if a person is over eighteen, we should not ask for their date of birth, but instead ask them to confirm that they are over eighteen (e.g. by ticking a box).

4. **Personal data must be kept accurate and, where necessary, kept up to date**

If we are collecting personal information, it should be kept up to date and accurate.

Example…
Where we maintain distribution lists of people's names, it would be a good idea to write to them once a year, so they can confirm that they should remain on the list and that their details are accurate.

5. **Personal data must be retained no longer than necessary**

We must not keep personal data for longer than we need it and we must also periodically review the data we hold and destroy it when we no longer need it.

Example…
We keep the names and addresses of people who attend day and evening courses for the length of the course and for a limited specified period after that to deal with any queries or issues that arise from that course. After that, the information must be destroyed in a secure manner.

6. **Personal data must used in a manner that ensures appropriate security of the personal data, including protection against accidental loss and destruction or damage**

We must ensure that we have appropriate security measures in place to protect the personal data we hold

Example…
We store personal information in a locked filing cabinet and ensure that if we need to move it, eg out of the office, it cannot be seen by others.

We destroy personal information by putting it in confidential waste bins supplied by the county council.

We ensure that when we are transporting records containing personal information it is locked away out of sight in our car.

We ensure that when we are carrying records we make sure that it is in a secure bag and can't be seen by others.

Your role in ensuring the security and confidentiality of personal information

You are a vital link in the chain

In your work with service users and customers of the council, you are likely to be responsible for use and storage of personal data. You have a personal responsibility to make sure that you handle personal information in a confidential and secure way. So, take a little time to look at the dos and don'ts below, about confidentiality and security and think about what personal information you handle in your job and how you can keep it secure

Confidentiality and Security at work ~ dos and don'ts

In your workplace	✓ Put confidential papers away safely after using them or when you leave your desk or working area ✓ Think about what is pinned up on notice boards ✓ Make sure that the recipient address on a letter or email is correct before sending it ✘ Don't send personal data via a text message or unsecured or personal email account ✓ When disposing of sensitive paper documents, make sure they are shredded or placed in waste bins marked 'Confidential'. ✓ If you want to dispose of any electronic media like a CD or memory stick, return it to ICT for secure physical destruction. ✓ Use the most secure way of passing on private or personal information eg avoid the use of faxes which can be read by anyone ✓ If you need to share personal information with another organization, check that the council has the authority to do so ✓ Hold conversations and phone calls about the public, customers and service users where you cannot be overheard and book meeting rooms where you cannot be overhead ✓ Personal information in electronic format should be transferred securely, eg in an encrypted email, or on an encrypted memory stick or an encrypted CD. ✓ If you are sending a spreadsheet (for example, in Excel), check for hidden information such as rows and columns ✓ In a video conference, ensure that participants cannot be overheard and, if possible, are wearing headphones ✓ Don't discuss confidential information with colleagues unless you are sure they have a need to know about it
Outside of work	✘ Don't disclose personal information obtained at work when you are at home, in the pub or anywhere else outside of work ✘ Don't disclose personal information in a conversation in a public

	place where you can be overheard ✘ Don't read documents on a bus, train or in a public place where somebody can look over your shoulder or view the information ✘ Don't leave papers or laptop on the seat of your car – lock them in your boot or take them with you ✘ Don't put any personal information obtained at work on Facebook, Twitter or any other social media (remember personal information can be anything that can identify an individual from that information and any other information in the public domain) ✘ Don't work on personal information on your own computer equipment ✘ Don't let family members and other people see personal records ✓ Respect things you hear in confidence at work
Data Breaches	✓ Always report any data breaches to your line manager as soon as you become aware of them and make every effort to put the matter right or reduce the harm caused by the breach

Procedures to help you

The County Council has a range of procedures to help you in ensuring that we handle personal information in accordance with the GDPR. Some of them are listed below:

- ✓ Acceptable Use of Facilities Procedure
- ✓ Clear Desk Clear Screen Procedure
- ✓ Data Breaches Report and Contain Procedures
- ✓ Mobile Phones and Text Messaging Procedure
- ✓ Printing, Posting Faxing Procedure
- ✓ Social Media Procedure
- ✓ Voicemail, Voice and Video Recording Procedures
- ✓ Working Away from the Office Procedure
- ✓ Working Securely in an Open Plan Office Procedure
- ✓ Confidential Disposal Procedure

Ask your line manager for further information about these procedures.

Now test yourself with the quiz below…

QUIZ ~ Data Protection and information security

These questions are to confirm your understanding of data protection and information security. **Please circle the correct answers and ask your manager to check them when you're finished.**

1. **Which of these are personal data?**
   Choose more than one answer
   - **A** List of all library users
   - **B** Database of addresses of Norfolk County Council libraries
   - **C** Details of a customer payments
   - **D** A paper list of colleagues' telephone numbers

2. **Norfolk County Council has collected names and addresses of residents in order to inform them of an environmental project in their area – which of these are acceptable uses of this information?**
   Choose more than one answer
   - **A** Sending Council leaflets about the project to these residents
   - **B** Selling the residents' details to other companies involved in the project
   - **C** Checking the accuracy of the residents' addresses by comparing them with a database of postcodes
   - **D** Sending the residents details of other events being staged by the Council

3. **If Norfolk County Council has some paper application forms containing personal data that are no longer needed, what should we do?**
   Choose one answer
   - **A** As the information is on paper, we can keep it in case a future use is found
   - **B** The paper forms should be securely disposed of, by shredding for example
   - **C** If the information is quite old, we can throw it away in a skip
   - **D** The information on the forms should be put onto a computer, and then we can keep it indefinitely

4. **You are at a reception desk, collecting customer questionnaires that include their name, address and a contact telephone number – what will you do when you take a break?**
   Choose one answer
   - **A** Leave them on the reception desk, as you don't think anyone will be interested to read them
   - **B** Hide them under other papers on the desk
   - **C** Lock them in an agreed safe place, out of view
   - **D** Ask a friendly customer to look after them while you take a short break

Any other questions?

Guidance for managers

1. Please discuss with the learner the answers to the questions throughout the workbook and in the quiz. Make sure that they understand any areas where they didn't get the correct answers.

2. If you would like a copy of the answer sheet for the Quiz, please apply to the Information Compliance Manager at information.management@norfolk.gov.uk

3. Fill in the final page of this workbook (Signatures ~ Data Protection and Information Security) and sign it together with the learner as a record that they have completed the workbook satisfactorily.

4. Ensure that the signed workbook is placed on the learner's file.

5. Ensure that name of the learner who has completed the workbook is placed on the department's central list with date.

6. Ensure that the workbook is competed every 2 years and follows steps 4 and 5 again.

Statement: Data protection and information security workbook

Name of employee:	
Statement: **Employee signature:**	I confirm that I have completed the data protection and information security workbook and understand my role and responsibilities in respect of data protection and information security at Norfolk County Council
Job role:	
Department:	
Date workbook completed:	
Line manager:	
Line manager signature:	
Date signed off as completed:	
Review date: (2 years from completion)	