Information governance for your small business

Information is vital to your business and it’s important to know how to handle it correctly. Everyone in your business is responsible for keeping information safe, protected and properly managed.

By developing good practices, you can help avoid simple mistakes and help keep information secure.

This training resource gives you basic principles to follow to make sure you fulfil your responsibilities. It’ll help you understand what your obligations are and what's expected of you.

|  |
| --- |
| Your feedback mattersThis training resource is in a testing phase and we welcome your feedback. We’ve written it with the needs of small businesses in mind. Please fill in our [survey](https://online1.snapsurveys.com/interview/59f74a7b-6b68-4f0f-b3e4-fe79e553f53e) to share your feedback on this resource.  |

# How this training resource will help you

This training resource is a practical support designed to help you protect the information that people have entrusted to your business. It’ll give you the tools you need to follow good practice and comply with data protection legislation. In the topics that follow, you'll find out:

* How to manage and account for the information you create and store.
* What you can do to keep all your information secure.
* How to spot requests for information.

We won't be able to cover every situation you might find yourself in, but we'll help you identify where problems might occur, and how you can help prevent these.

Topics we’ll cover:

* [Why information governance is important](#_Why_information_governance)
* [Managing information](#_Managing_information)
* [Information security](#_Information_security)
* [Transparency and trust](#_Transparency_and_trust)
* [People’s data protection rights](#_People’s_data_protection)
* [In summary](#_Your_most_valuable)

# Why information governance is important

Customers, stakeholders and colleagues share their personal information with your business. They must be able to trust that you’ll keep it safe, and only use it in ways they expect.

Think about the different types of information you come across in your role. What would be the risks if that information was lost, corrupted or shared inappropriately?

Knowing what the risks are will help you identify ways to prevent problems. You may be in the best position to identify potential risks in relation to the information you handle. Don’t keep these risks to yourself – raise them with an appropriate person in your business so you can decide what steps you can take to reduce incidents. Identifying and taking action to mitigate risks before they happen will save your business time, money and reputational damage.

There are many ways personal information could be put at risk.

How would you feel if this was your personal information?

|  |
| --- |
| ScenarioA care worker was chatting with his friends in a busy coffee shop. He told them how annoyed he is that June, an older adult, has been left vulnerable to attack. June lives alone in a ground floor flat, but the housing company haven’t fixed her broken door lock, despite repeated requests. A number of customers in the coffee shop overheard the care worker’s remarks and now know June is an easy target for thieves.  |

|  |
| --- |
| ScenarioMina fell over at work. The security guard shared CCTV footage of her fall with several of Mina’s colleagues. One of them videoed the footage on his phone and later shared it on social media because he thought it was funny. Mina feels humiliated and upset. |

|  |
| --- |
| ScenarioGordon’s manager read through Gordon’s occupational health assessment report while on the train. The laptop screen could be seen by at least three other passengers. They were able to read the report, which included details about Gordon’s mental health issues. |

|  |
| --- |
| ScenarioThe mortgage advisor attached Gethyn’s completed financial assessment document to an email, but accidentally sent it to another client. That person now knows about Gethyn’s credit card debts. |

|  |
| --- |
| ScenarioA hotel’s online payment system wasn’t working, so Melanie gave her card details over the phone. The receptionist wrote the card details, including CVV, on a piece of paper and left it on the desk while she went on her break. When she returned there were a number of guests standing by the desk, waiting to check in. One of them had photographed the paper with the card details on it. |

# Managing information

Information is one of your most valuable assets, so you have to look after it and be accountable for it. We all need to take personal responsibility for managing the information we create and use on a daily a basis.

You can demonstrate your accountability by keeping good records of the information you hold, what you do with it and how you comply with the law.

Keeping good records means you’re always able to find what you need, and you’ll know that the information is up to date.

## What role do you play?

Good information management helps you work more efficiently and find the information you need to do your job.

Save information in the right place so others can find it

* Is all the information you handle saved in the correct place?
* Can you find it easily? Could others find it easily if they didn't have you to ask?
* Do the appropriate people have access to where the information is stored?

Label your documents clearly

* Does the name of your document or folder actually tell you what's in it?
* Would another member of staff know what the folder or document was, just by looking at the title?

Store personal information securely

* Does your storage have effective security measures in place, such as locks for physical document storage and passwords for sensitive electronic files?
* Can information only be accessed by people who need to see it?

Dispose of information securely when you no longer need it

* Do you regularly review your documents to see if they're still necessary to keep?
* Do you know how to dispose of information securely?
* Are you aware of how long you should keep documents for?
* Is the information you're storing out of date or inaccurate?

## Why keep good records?

Look at the following scenario and answer the questions in the exercise.

|  |
| --- |
| ScenarioI’m Bailey. I've been working as a clerk at a firm of solicitors for three years now. I mainly deal with filing correspondence and photocopying, but sometimes I have to find information to comply with court orders or client requests.Three weeks ago, the practice manager asked me to find all the information we have about a former client who’d asked us for a copy of his case. The deadline was one calendar month.I soon discovered the last person who'd worked on the client’s file had left the company a few months back.We keep all our files on our casework system. Paper documents are scanned to the system when a case is completed, so everything is in one place and the file can be closed. That was the first place I looked.There was an file with the client’s name on. However, the documents in it had filenames like 'Document 2' and 'Notes made on the 2nd March', which didn't follow our file-naming conventions. I had to open each one and go through it, which took a long time.And when I opened these documents, they were just vague notes from a phone call. The notes were very brief and there wasn’t a clear record of the information provided. Also there wasn't anything to tell me where else to look. It was an incomplete picture of the case.I thought that maybe the information had been kept somewhere else, and the previous filing clerk hadn't got round to saving them to the right client system. A colleague thought there were some documents still left in the clerk’s desk drawer and also recalled notes of a client meeting being sent by email in March.I did find a bundle of papers in the drawer eventually but with only a day to spare. I couldn’t find the meeting notes and I’m worried our records about this case are incomplete. The client won’t be happy if we don’t give him all the information he’s asked for. |

|  |
| --- |
| ExerciseWhat went wrong in Bailey’s scenario?Why do you think Bailey couldn’t find the information they needed? * They were looking in the wrong place.
* The information wasn't saved where it should have been.
* They didn't know what they were looking for.
* The documents were poorly named.
* When the filing clerk left, they didn’t tidy up their records.
* Documents were left in a desk drawer, rather than being scanned and filed appropriately.
 |

In this case there are a number of factors which have contributed to the problem:

* The information wasn't saved where it should have been.
* The documents were poorly named.
* When the filing clerk left, they didn’t tidy up their records.
* Documents were left in a desk drawer, rather than being scanned and filed appropriately.

The clerk hadn't kept good and complete records on the corporate systems. This meant that Bailey struggled to find what they needed and may not have fully complied with the client’s request.

Additionally, if the case files had been lost then this could be a breach of security.

You should always move your records to your relevant storage systems as soon as possible. You should allocate yourself time to do this on a regular basis.

## Naming your documents

It’s time-consuming to have to open every file and folder every time someone at your business needs to find some information.

Using a document naming convention can make it easier for you and everyone else to search for, retrieve and understand the information you have.

|  |
| --- |
| ScenarioYou can’t tell what’s in these files without opening them: Stats 01/01/22 JC/CH When you open the files, they turn out to be:* spending reports that were needed for the annual report;
* minutes of a meeting with a potential investor; and
* detailed notes about the decision to restructure a department and reassign managers.
 |

Good practice

Use titles that descriptive and consistent so that it’s clear what the files contain. You can tell what’s in these files without opening them:

Stationery invoices 21-22

Clarke investment meeting minutes 01/01/22

HR reshuffle plan 9-19 v0.2

Here are some general principles to follow:

* Keep filenames short, clear and meaningful.
* Use a consistent and logical approach – order the name of a file in a way that makes it easiest to retrieve, for example by date or client name.

You should follow your naming convention for all documents and emails.

The key thing is to be consistent with your colleagues.

You should also consider including dates or version numbers in your file names, so you know you’re looking at the latest information.

File names should include enough information for you to be able to identify what’s in a file, and whether it’s the most up-to-date information. This will help you find what you’re looking for easily, and make sure you’re always using the most current information.

## Handling instructions

It can be helpful to mark documents with handling instructions when appropriate. These can be particularly useful when sharing information by email. Providing clear handling instructions to those you share information with helps maintain confidentiality.

Examples include:

* For HR use only – this information should only be shared with HR colleagues.
* Do not share further – the information is for your eyes only and should not be shared.
* Consult the originator before sharing – you may be able to share this information but you first need to check with the person who created it.

# Information security

All your information must be held and handled securely, and this applies to both your electronic and hard copy information. Regularly protect your system with available security patches or updates from the manufacturer to keep it as secure as possible.

You also need to keep your hard copy information secure within your own buildings and when you're on the move.

## What is information security?

Information security is about protection of information including personal data.

Its main focus is protecting the confidentiality, integrity and availability of information.

Confidentiality

* Confidentiality is about protecting your information from unauthorised people or processes. The risk to your electronic or hard copy data includes laptop theft, paper theft, password theft, or sensitive emails being sent to the wrong people. It also includes confidential information being talked about in a public space.

Integrity

* Integrity means protecting information from unauthorised changes, for example someone abusing their system access to delete or edit something without the appropriate authorisation.

Availability

* Your information must be available to authorised users when it's needed. For example, being able to access your systems and email and preventing service disruptions due to power outages, hardware failures or system attacks upgrades.

## How you can protect information

Think about what you can do to protect information in your role.

If something goes wrong or nearly goes wrong, no matter how it happened, report it as a security incident.

Here are some security tips that may be relevant in different working environments.

Working in the office

* Don't allow anyone to follow you through secure doors or into non-public areas where they’re not supposed to be.
* If you do have visitors to private areas in your premises, stay with them, or make sure you know where they are. Be aware of what’s visible in the areas they pass through and make sure they wear visitor passes so other staff members know who they are.
* If relevant, wear your ID badge at all times and if you lose it, report it immediately.
* Don’t leave personal information where people who don’t need to access it may see it. It’s particularly important to clear information from your desk whenever you leave the office, for example at lunchtime or the end of the day.
* Lock your computer screen when you leave your desk.
* Store paperwork in a locked filing cabinet.
* Dispose of paper documents using confidential waste bins or cross-cut shredders.

Working on the move

* Be aware of who can see your screen or hear your conversation.
* When using public transport, take a minute to check you have everything with you before getting off at your stop.
* Wherever possible, only use secure WiFi networks.
* Take care when disposing of documents. If you can’t dispose of them securely while you’re away, keep hold of them and dispose of them through your confidential waste system when you return to your business premises.
* Add extra security to your devices, such as two-factor authentication or encryption.
* Only take the documents you need. Don’t take the entire file if only one form is relevant.
* Be aware of and abide by your business’s remote working policy.

Working from home

* Be aware of who can see your screen or hear your conversations.
* If other household members have access to your devices, store business data in a secure folder, protected by a strong password.
* Keep paper documents in a locked storage cabinet.
* Don’t put paper documents in your ordinary household waste or recycling bin. Use a cross-cut shredder to dispose of them securely.

Other useful security tips

* Keep your IT security up to date by regularly installing security updates.
* Always use appropriate redaction software when redacting electronic information.
* Use blank template documents and store them separately from completed documents.
* Keep your contact details up to date.
* Back up your systems.

## Using email

We use email for so many of our important communications, especially with remote working. But it’s vitally important to take care when you’re sending information in this way. For example, mistakes like emails being sent to the wrong person or with the wrong document attached can be both costly and reputationally damaging.

Here are some useful tips for you to consider.

Disable autofill

Some email systems auto-generate a recipient address when the first few letters have been typed. This might seem like a time-saving device, but it can also cause problems.

|  |
| --- |
| ScenarioYou’re sending a final payment reminder to John.smith@business.com. You type ‘John’ and your autofill selects ‘John.brown@orgmail.co.uk’. Without noticing this you send the email, and John Brown receives information about John Smith’s failure to settle his invoice. John Smith will not be happy that you’ve shared information about his debt and John Brown will think you can’t be trusted with customers’ information – that’s potentially two customers you’ve lost. Not to mention the reputational damage if they tell other people what happened, and the time you have to spend dealing with the issue and apologising. |

Instead, copy and paste email addresses into the address bar, and make sure you check them again, before pressing send.

Check attachments

This is another occasion when your clear naming policy is useful. If your documents are clearly named, you’re more likely to spot immediately if you’ve attached the wrong one in error.

Make sure the file you attached is the one you want to send. Add extra protection to sensitive files by protecting the document with a password and sending the password to the recipient by another method, such as messaging. That way, if the email does go astray, the incorrect recipient can’t open the document.

Know who you’re replying to

It’s not always necessary to ‘reply all’ to every recipient in an email thread. Not everyone on the previous distribution list will need the information you’re sending.

Check the chain

If you’re forwarding an email, check if it has other communications below it. Check what’s in the previous emails to make sure you’re not sharing information you shouldn’t be.

Don’t use your email system as a storage area

If you need to keep information, move it to a storage area and label it clearly. Keeping information in your inbox makes it harder to find, and there’s greater potential that it’ll be accidentally deleted, particularly if you have an automatic deletion period.

Don’t keep emails you no longer need

If you don’t need something, delete it. This will free up storage space and reduce the amount of information you’ll need to search through if someone makes a subject access request (SAR). It’ll also reduce the amount of information that could be compromised if you were the subject of a cyber-attack. It’s a good idea to have an appropriate automatic deletion period, for example 12 months, after which the system will delete any email that hasn’t been marked for preservation.

## Passwords

To keep your passwords safe, you should never share your password – this increases the risk of an unauthorised person seeing or reading personal data.

Make sure you keep personal and work passwords completely separate, so a personal one can’t be used to guess a work one.

What to consider when creating a password

* Choose a password that’s difficult to guess but easy for you to remember – something that's personal to you and only you would know. In general, the longer the password is the harder it is to crack.
* Don't recycle passwords.
* Try turning a sentence into a password, eg "My first house was number 120 " becomes "mfhwn120". Alternatively, create a passphrase by using three or more random words, eg "correcthorsetomato".
* Avoid using the same password for multiple accounts. If one is compromised all are compromised.
* Use a combination of characters – upper and lowercase, numbers and punctuation.

## Suspicious emails

There may be attempts to send you emails that contain viruses or links to other malicious sites which could infect your systems or steal your data. If you have anti-virus software installed most of them get should stopped before they get through. However, you may still receive suspicious emails, and you need to be alert to them. Some are very convincing and targeted.

Here are some useful tips for you to consider.

How to spot a suspicious email

It’s common for malicious emails to be:

* unexpected;
* sent from someone you don’t recognise;
* given generic subject lines such as ‘invoice’;
* contains links in the body of the email; and
* urgent – the sender will try to make you act quickly.

If you’re not sure whether the email is genuine, or if it comes from an organisation you don’t recognise, you should avoid replying or clicking on any link as this might confirm your email is live and make you a target for more spam emails.

Remember, if the email feels suspicious, unexpected or unusual you should report it.

What to do if you spot a suspicious email

If you’ve received an email you think is suspicious:

* don’t open it;
* don’t click on the links or open attachments;
* don’t forward it on to colleagues or externally – not even to your IT support;
* report it immediately to your IT support or manager, as appropriate (eg using the ’Report Message’ button that may be in your email toolbar); and
* delete the message from your deleted or junk folder.

Avoid using your work email address to sign up for anything that isn't work-related. This could help reduce potential email attacks.

## What might go wrong?

|  |
| --- |
| ExerciseWhich of these do you think pose an information security risk?* Sharing a password
* Leaving a bundle of papers on a train
* Sending an unencrypted disc or USB
* Not keeping your devices updated
* Not checking recipients' contact details
* Not recognising suspicious emails
 |

The answer is: all of them.

All these things are easy to do. Some are riskier than others, but avoiding them helps to maintain the security and confidentiality of the information you hold. You are the first and strongest line of defence against risks to your information and property. By following a few simple security measures, you can help prevent these security incidents.

Here are some tips:

* Take time to think about what you’re doing.
* Don't be rushed or take shortcuts.
* Check before you share or disclose anything.
* Report any suspected or actual security incidents to your manager immediately.
* If you're unsure, ask your manager or IT support.

Our [SME web hub](http://www.ico.org.uk/hub) contains tips and advice to help develop good security practices at work.

Knowing how to securely handle information is important. A breach of security can lead to serious consequences for everyone, so understanding how information can be vulnerable in your job role is crucial.

## Report security issues quickly

Some personal data breaches must be reported to the ICO within 72 hours of you finding out about them, so it’s essential you raise any incident as quickly as possible.

If you lose something like a mobile device or ID badge, even if you think the loss is only temporary, report it to the relevant person in your business. Don't delay reporting the loss because the potential consequences for the business, and you personally, can quickly escalate.

And don't be afraid to report security issues to your manager or appropriate person in your workplace, including near misses – even if you think you're the one who's made the mistake. It may not turn out to be an incident, but you learn a lot from near misses. The incident will be much harder to manage if you delay – or worse – don't say anything.

## Do we still need the information?

It's crucial you keep important information, but at the same time you need to effectively manage redundant or outdated information. Your business should have appropriate retention periods, ideally set out in a retention schedule. This says how long you should keep certain types of information and helps you make sure information is managed and securely disposed of without delay.

You may need to keep different types of information for different lengths of time, in accordance with legal obligations and industry standards. For example, you might want to keep customer order forms for six months, in accordance with your returns policy, but invoices for a longer period in accordance with any applicable financial regulations.

Through regular housekeeping activities you should review and delete information that’s no longer needed. For example, you may not need to keep details of customer orders after they’ve been fulfilled, or copies of a quotation that has expired.

It's important you can show your information is accurate and up to date and you're not keeping it longer than you need it.

This is especially important for personal data, including personnel files.

Regularly review records containing personal information so that if you no longer need it, you can delete it.

## Secure disposal

The right method of disposal is key.

|  |
| --- |
| ExerciseWhat do you think are suitable methods to dispose of paperwork?* + Confidential bin and disposal service
	+ General wastepaper bin
	+ Cross-shredder
	+ Recycling bin
 |

You should consider using a confidential bin and reputable disposal service or a cross-shredder once something is no longer needed.

Never put work papers into general waste, recycling bins, public bins or your bins at home.

Ask if you’re not sure whether something is still needed and if required, update the record to show that it has been disposed of.

# Transparency and trust

Transparency is vital to ensure you have the trust of your customers, clients and staff.

You must normally provide people with certain information about your collection and use of their personal data. This privacy information could be displayed on your website or in your offices. Keep this privacy information accurate and up to date by reviewing it on a regular basis.

Publish your privacy information, and make it available as early as possible whenever anyone contacts you or you contact them. Make sure you do what you say you will with their personal data.

# People’s data protection rights

Data protection gives us all specific rights to ask about what’s being done with our personal data.

You need to be aware of these rights and able to recognise if somebody has made a request relating to them – in most cases the business will have to reply to the request as quickly as possible and normally no later than one calendar month of it being received

Rights requests can be made verbally and in writing. If you’re not sure if it’s a request, consider checking with the requestor to confirm what they want or visit our [SME web hub](http://www.ico.org.uk/hub) for advice.

People have the right to access their own information

If you hold personal information about someone, they’re entitled to ask you for copies of that personal information and other supplementary information. This is known as a SAR.

People have the right to be informed about what you're doing with their personal data

If someone asks about how your workplace handles personal information you could, for example, direct them to your business’s privacy notice. Alternatively, you could send them a copy or read it to them.

People have the right to ask you to erase their personal data

This is also known as the right to be forgotten. If someone asks you to erase their personal data and you have no legitimate reason to continue to keep it you need to erase it. Let them know what action you’ve taken.

People have the right to have their data corrected if it's inaccurate or completed if it's incomplete

This is known as the right to rectification. For example, a customer might ask you to update their contact details.

People have the right to object to you processing their personal data

If someone doesn't think you should be processing their personal data, they can ask you to stop. People have an absolute right to stop their personal data being used for direct marketing – there are no exemptions to this or grounds for you to refuse.

People have the right to data portability

This allows people to move, copy or transfer personal data easily from one IT system to another. For example, this could be electricity meter reading history.

People have the right not to be subject to a decision based solely on automated processing

This relates to processing where there’s no human input and which has a significant effect on people. You have to inform them if they are subject to it and give them the option to request human involvement. You need to assess the impact to people before doing any automated decision making and take steps to reduce the risk of errors and discrimination.

People have the right to request restriction or suppression of their personal data

This relates to the restriction of personal data and limiting its use, especially where the accuracy or use of the information is contested, or they object to the processing.

It’s important to be aware there are circumstances when these data protection rights don’t apply. For example, you can’t object to your employer sharing your wage information with HMRC because they have a legal duty to do so. There’s more information about when these rights apply on our [website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/).

## Requests for information

If you work for a public authority you’ll need to respond to requests made under the Freedom of Information (FOI) and the Environmental Information Regulations (EIR).

If your business carries out tasks on behalf of a public authority, you’ll need to pass FOI or EIR requests onto the authority you work for. These are laws that give people the right to ask for official information from public authorities. If this applies, the public authority has 20 working days to respond.

Act quickly when you spot a request

If you receive an information rights request, such as a SAR, or an FOI or EIR request you need to act quickly because there are set time periods for responding. Make sure you tell the appropriate person in your business, such as your data protection lead or manager.

Be alert: requests may not be clearly labelled by the person making them. They may be contained within another piece of correspondence. FOI requests must be made in writing, but personal information rights and EIR requests can be made verbally.

If you receive a verbal request, it’s important to make a written note of what the requestor has asked for, their name and contact details, and any other relevant information, such as their reference number. It’s also a good idea to ask them what they want to receive, which could narrow down your search.

Requests can be sent to anyone in your business.

* Read all the correspondence you receive and check for information requests – they might not all be obvious.
* Listen to customers on the phone – they may be making a verbal request for information.
* Act quickly – failing to follow strict timescales can lead to a breach of the law and complaints.

Do not obstruct transparency

It could be a criminal offence if you try to prevent the disclosure of information that has been requested under freedom of information or data protection laws.

When a request is received, any information relevant to the request that you hold at that time, must not be:

* + altered;
	+ defaced;
	+ blocked;
	+ erased;
	+ destroyed; or
	+ concealed.

You could be personally liable if you do.

Remember that information you hold and information you create on behalf of your business could be disclosed.

This might include:

* + draft documents;
	+ meeting notes that you made quickly and meant to delete;
	+ the email you sent to your manager about a frustrating complaint; and
	+ the letter you sent to a stakeholder explaining you don't think their new idea is a good idea.

Embarrassment isn’t an exemption so when you’re writing documents or emails remember they could potentially be disclosed.

# In summary

Information is one of your most valuable assets.

Through good information management you can help get the right information to the right people, and keep it no longer than you need it.

This helps avoid reputational risk, saves time and guarantees the information you have is reliable and up to date.

Keeping good records of the work you've done and the decisions you've made helps to show your accountability, and demonstrates to others how you’re meeting your legal obligations.

Remember to:

* Think privacy at the beginning. What is the privacy and security impact of what you want to do?
* Label all your documents clearly.
* Save information in the right place so others can find it.
* Dispose of information securely when the applicable retention period expires.
* Get rid of redundant or outdated information.
* Familiarise yourself with your corporate standards and any local information management practices in place.

|  |
| --- |
| Your feedback mattersDid you find this training resource for small businesses helpful? Please fill in our [survey](https://online1.snapsurveys.com/interview/59f74a7b-6b68-4f0f-b3e4-fe79e553f53e) to share your feedback on this resource. We welcome your feedback as we continue to make improvements.If you have any questions you can [get help and support from the ICO.](https://ico.org.uk/for-organisations/sme-web-hub/get-support/) |