



Information Security Month **October 2025**



Newsletter 4 | Records Management

Welcome to the fourth of five newsletters which will be shared with you during October to mark Information Security Month.

Information Security Month is an international initiative aimed at raising awareness about cyber security threats and educating individuals and organisations on how to protect themselves.

The theme of this week's newsletter is Records Management.

Secure records management is a vital part of Information Security Month because protecting records - whether paper or digital - helps prevent data breaches, identity theft, and misuse of sensitive information.

By managing records securely, organisations ensure compliance with the law, protect personal information, safeguard trust, support efficient working and reinforce the wider culture of information security.

This newsletter is a simple guide to what records are, why they matter, and how to manage them safely.

In this newsletter you'll learn:

- ▶ What a record is
- ▶ Why it's important to know what records you keep
- ▶ How to check how long you should keep records for
- ▶ How to keep records securely
- ▶ Where to send paper records that should be retained but that you no longer need in the office/station.
- ▶ How you should delete and destroy records that are no longer needed.

Making Cumbria a safer place for all



What is a record?



A record is any piece of information created, received, or kept as part of your job that provides evidence of what we do as a service.

It doesn't matter what format it's in - paper or digital, formal or informal - if it documents decisions, actions, or transactions, it's a record. Not all information is classed as a record - e.g. user manuals for equipment. If you aren't sure then you can ask Information Governance.

Where you might find records:

Physical records



Paper files, notebooks, letters, printed reports, maps, photographs, receipts.

Digital records



Emails, spreadsheets, Word documents, PDFs, databases, case management systems, Teams chat logs, photos or video files.

Other formats



Voicemails, texts or WhatsApp messages (if used for CFRS business), CCTV footage, recordings of meetings.

What to look for when identifying records:

- ▶ **Evidence** – does it record a decision, action, or policy?
- ▶ **Accountability** – could it be needed to demonstrate how we reached a decision or to answer a query from the public, auditor, or regulator?
- ▶ **Legal/Business need** – is it required by law, for service delivery, or for safeguarding reasons?

Top Tips:

✓	Don't assume only "official" documents are records – notes, drafts, and messages can all count
✓	Ask yourself: "Would someone need to see this in the future to understand what we did and why?" If yes, it's a record
✓	Keep CFRS records in the correct place (on official systems, rather than personal drives, or personal Laptops/ smart devices).



Why it's important to know what records you keep



Whether it's a paper file in a cabinet or an email stored on your computer, every piece of information we create or handle in our roles can be part of the service's records. Knowing what records you keep – and why – and for how long are the foundation of good records management.

Why it matters:

Legal duties



Under laws like the **Data Protection Act 2018** and the **UK GDPR (General Data Protection Regulation)**, we must know what personal data we hold, where it's kept, and how it's used. This also helps us respond quickly to **Subject Access Requests (SARs)** (when someone asks to see the information that we hold about them).

Transparency



The **Freedom of Information Act (FOI)** gives the public the right to request certain records. If we don't know what we have, we can't respond properly.

Efficiency



Keeping track of records avoids duplication, wasted storage space, and time spent hunting down missing files.

Security



If we don't know what we have, we can't protect it. Unmonitored records are at higher risk of being lost, stolen, or accidentally shared.

Top Tips:



Keep a simple list of the main records you work with, where they are stored, and how long you should keep them.



Don't keep records "just in case" – only hold onto what you need for legal, business, or statutory reasons.



You should look up how long to keep records on the **CFRS Retention and Disposal Schedule** or ask Information Governance at **InformationGovernance@cumbriafire.gov.uk**



Remember: a "record" isn't just paper – it includes emails, spreadsheets, databases, photos, videos, and even Teams chat logs.



CASE STUDY

When records go wrong

Here's a real-world example that shows why records management really matters:

University Hospitals Coventry and Warwickshire Trust – Records found in public waste bins.

Two incidents

In one, medical records were found in a communal waste bin at a residential block; in another, in a bin outside the hospital. The papers included details of patients' medical procedures/test results. The ICO found this breached Data Protection law and censured the Trust.

theguardian.com/healthcare-network/2011/oct/27/ico-university-hospitals-coventry-warwickshire-trust-data-loss

Lesson learned:

Never dispose of paper records in ordinary rubbish. Always use secure shredding or confidential waste services.



How long you should keep records for

We are legally required to keep some records for a set time – for example, financial records or adoption case files. Other records are kept for a specific time for business reasons. All records should be listed on the CFRS Retention and Disposal Schedule. If any records are missing from this, contact Information Governance - InformationGovernance@cumbriafire.gov.uk.

Keeping records too long increases risks (data breaches, information leaks) and makes it harder to find what you actually need.

Top Tips:



Always check the **CFRS Retention and Disposal Schedule** – it tells you how long different types of records should be kept.



Once a record has reached the end of its retention period, it should be destroyed as confidential waste or deleted if they are digital records..



If you're unsure, contact Information Governance for advice.



Where you should send paper records that need storing



If you have physical records (like paper files) that you no longer need to use day-to-day but must keep for legal or business reasons, they should not be left in your desk or office.

These records must be sent to **Records Management Service**, who store and track them securely.

Top Tips:

- ✓ Don't store old files at home, in cupboards, or on shared drives that no one manages.
- ✓ Contact recordcentre@cumberland.gov.uk with a list of the paper records you'd like to transfer to them and wait to hear back. You should use the "records transfer form" on the hosted Service's **Records Management** intranet site [Data Protection, Security, Records Management and Freedom of Information](#)
- ✓ Always label records clearly so they can be retrieved quickly if needed.

How to delete and destroy records that are no longer needed



Once a record has reached the end of its life, it must be disposed of properly. Simply dragging a file to the "Recycle Bin" on your computer isn't enough – it may still exist in backups. Similarly, shredding is the only safe way to destroy paper records.

Top Tips:

- ✓ **For paper records:** always use the Service's **confidential waste bins/sacks**. Never put any CFRS records in the normal rubbish or recycling. The Service has a contract with an external company who carry out confidential waste shredding to specific standards that meet Information Security requirements
- ✓ **For digital records:** always double-check before deleting – make sure they have reached their retention period, and the records are not subject to an ongoing request (such as a FOI or Subject Access Request).
- ✓ Remember, keeping records for too long may conflict with Data Protection legislation, but destroying records prematurely can also lead to problems.





Send us your comments and feedback

Share your comments and feedback with us, including any suggestions for how information security could be improved, or an example of good Information Security practice from a colleague, or team.

The best examples will be included in our fifth and final newsletter at the end of the month.

Send your comments, suggestions and examples of good Information Security practice in an email with the subject line **“Information Security Month Feedback”** no later than Friday 24 October to security@cumbria.fire.gov.uk and remember to include your full name and contact details.



Thanks for reading this far! The theme of next week's newsletter will be Information Security – Do you know who's in your meeting?

In the meantime, contact Information Governance for advice if you're unsure about anything related to the management of records.



InformationGovernance@cumbriafire.gov.uk

#StrongPasswords **#CyberAware** **#BrowseSafe** **#ThinkCyber**
#MindfulClicks **#OwnYourSecurity**

How to keep records secure



Records must be protected at all times, whether paper or digital. Breaches can result in fines, loss of public trust, and harm to the people whose data is exposed.

Top Tips:



Lock away paper files when not in use – don't leave them on desks or in cars



Never share records with people who don't have a genuine business need to see them.



Use strong passwords and multi-factor authentication for digital systems.

CASE STUDY

When records go wrong

Here's another real-world example that shows why records management really matters:

Government files left on a train

In 2008, top-secret government documents on terrorism and organised crime were left on a commuter train in London. A passenger handed them to the BBC, who reported the breach. The event caused major embarrassment, raised security concerns in Parliament, and damaged public confidence.

theguardian.com/uk/2008/oct/28/terrorism-security-secret-documents



Lesson learned:

Physical records must be kept secure when in transit. Never carry sensitive documents loosely in public.



Who to contact with questions



If you're ever unsure about records management – how long to keep something, how to store it, or how to delete it – don't guess.

Information Governance is here to help.



informationgovernance@cumbriafire.gov.uk

Remember

Good records management is not just about staying organised – it's about protecting people, complying with the law, and keeping public trust.

