Cumbria Fire & Rescue Service

Information Security Month October 2025

Newsletter 2 | Data Protection - Be data smart

Welcome to the second 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 Data Protection – Be data smart. In this newsletter you'll learn:

- The do's and don'ts of accessing personal data
- How to identify, report and prevent data breaches
- How to be data smart
- What training and support is available.

Accessing Personal Data - Do's and don'ts

Accessing personal data is a privilege that comes with responsibility. Every action you take reflects our approach to protecting the privacy of any person using our services. We should all work together to uphold the highest standards of data security and compliance.

The list below includes guidance on accessing personal data and is designed to reinforce Cumbria Fire & Rescue Service's commitment to data protection, privacy, and secure handling of personal data sensitive information.

Do's

- ✓ Ensure you have a clear lawful basis for accessing personal data
- ✓ Inform individuals how their data is used via privacy notices
- ✓ Access only the data necessary for your task
- ✓ Keep personal data accurate and up to date
- ✓ Use secure systems and protect data with passwords/encryption
- ✓ Store data only on authorised platforms
- ✓ Dispose of data securely when no longer needed
- ✓ Respond to Subject Access Requests within one month
- ✓ Report data breaches promptly to your DPO
- ✓ Take extra care when working remotely or offsite.

Dont's

- ✗ Don't access data without a valid reason
- ✗ Don't share data without consent or legal basis
- ✗ Don't retain data longer than necessary
- ✗ Don't include unprofessional comments in records
- ✗ Don't use personal devices or unauthorised services
- ✗ Don't email sensitive data without encryption
- ✗ Don't display personal data in public or shared spaces
- ✗ Don't assume consent - always verify and record it.

If you have a question, contact your Data Protection Officer (DPO): **informationgovernance@cumbriafire.gov.uk**.

Data Protection by Design and Default

The importance of embedding Data Protection by Design and Default into all CFRS projects and system changes is becoming more apparent.

In some cases, data protection is considered too late - often during implementation, leading to delays, rework, additional/unseen costs and compliance risks. The lesson? Data Protection must be part of the conversation from the very beginning.

When starting a new project or making changes to systems or processes, always ask:

- *Will personal data be used?*
- *Will the use of data have any impact on people?*

By identifying these issues early, project teams can build in the necessary safeguards and ensure compliance with data protection principles. Waiting until a project is well underway may mean it's too late to make important changes.

Thinking about data protection at an early stage saves time, reduces risk, and ensures that personal data is secure and protected at all times.

At the very least you should use a Data Protection Impact Assessment to identify, mitigate and manage risks.

Contact Information Governance to find out if a DPIA is required for a project: **informationgovernance@cumbriafire.gov.uk**.

Identifying, Reporting, and Preventing Data Breaches

Data breaches aren't just IT issues - they're business risks. Prevention starts with awareness, and response starts with readiness. Let's stay vigilant, informed, and proactive.

This briefing outlines how to recognise, respond to, and proactively prevent data breaches. It supports our commitment to safeguarding personal and sensitive information, ensuring compliance with regulations like the UKGDPR, and maintaining trust with stakeholders.

Identifying a Data Breach

A data breach occurs when personal or confidential information is accessed, disclosed, altered, or lost without authorisation. Breaches can be:

- confidentiality breaches – e.g. unauthorised access or sharing of data
- integrity breaches - e.g. unauthorised modification of data
- availability breaches - e.g. accidental deletion or loss of access to data.

Common Signs of a Breach:

- unusual system activity or login attempts
- missing or corrupted files
- reports of phishing or social engineering attempts
- devices lost or stolen containing sensitive data
- data sent to the wrong recipient.

To report a data breach contact Information Governance as soon as you become aware of the breach: **informationgovernance@cumbriafire.gov.uk**.

If you're reporting a data breach please provide as much information as possible, this should include (but not be limited to):

- what has happened
- where it happened
- who is affected
- who caused it i.e., named officers
- what has been done to contain it
- supporting material that provides evidence of actions taken.

Top Tips for Prevention:

****	Use strong passwords
0101 0101	Encrypt sensitive data sent by email using egress or password protection
	Manage who has access to data and review permissions on a regular basis
	Complete training on a regular basis (request a session if you have specific needs)

If you have a question contact your Data Protection Officer (DPO): **informationgovernance@cumbriafire.gov.uk**.

CASE STUDY

Data Breaches – Think Before You Hit Send

Meet Rachel, a busy Officer working on a tight deadline. One afternoon, she needed to send to send sensitive information about a member of the public to her colleague John Smith. She quickly typed "John" into the Outlook address bar, and without double-checking, because she regularly contacts John Smith, Rachel hit send.

Moments later, Rachel realised the email had gone to John Bloggs, a completely different staff member. The autofill feature had selected the wrong recipient, and a data breach had occurred.

This kind of mistake is becoming increasingly common. Autofill in Outlook can be helpful, but it also poses a risk when handling personal or sensitive data.

How to Avoid This:

- Go to **File > Options > Mail >Send Messages** and click **Empty Auto-Complete List** on a regular basis.
- Use the Outlook directory to find the correct email address.
- Type the full email address manually if you're unsure.
- Always double-check the recipient before pressing send.

Rachel reported the breach immediately, but the incident serves as a reminder: **slow down and check before you send**. A few extra seconds can prevent a serious data protection issue.

Being Data Smart...

Data Protection isn't just an IT issue - it's a shared responsibility. Completing your training is a vital step in protecting our organisation, the communities we serve, and yourself. Let's stay informed, compliant, and secure, but most importantly let's work together to become data smart.

Training is important as it supports:

Legal and Regulatory Compliance

Under the UKGDPR and other data protection laws, CFRS must be able to demonstrate accountability – including staff training as a core requirement. Failure to provide training can result in fines, audits, and reputational damage.

Trust and Reputation

Customers, partners, and regulators expect CFRS and its employees to handle data responsibly. A well-trained workforce builds confidence in the ability to protect sensitive information.

Risk Reduction

Completing training means that you are more aware of poor practice that could cause breaches, you are less likely to be a victim of phishing/social engineering attacks but most importantly you can encourage others to be data smart.

Empowerment and Accountability

Completing training will provide knowledge and confidence to make informed decisions, report incidents, and uphold privacy standards. It ensures everyone understands their individual responsibilities in protecting data.

Top Tips for Prevention:

Complete Training Promptly – don't delay; training is time-sensitive and mandatory

Engage Actively – ask questions, take notes, and apply what you learn

Stay Updated – refresh your knowledge regularly; policies and threats evolve

Lead by Example – encourage colleagues to take training seriously and follow best practices.

What training options are there?

- Information Security and Data Protection eLearning - If you haven't already, please log into Learning Pro now to complete the training course.
- If you wish to arrange ad hoc Data Protection training for your team, delivered by our Information Governance Officer, please contact: **informationgovernance@cumbriafire.gov.uk**.

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 – Think before you click!

In the meantime, if you have any questions, please send them to: **security@cumbriafire.gov.uk**.

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