Welcome to our Seminar
Empowering the Future of Housing

chess® Making it Easy to work **Securely, Anywhere, Anytime**

Securing Housing Data with Microsoft Purview

Robert White
Lead Consultant

"Making it easy to work securely anywhere, anytime"

Microsoft Purview Information Protection

How information protection can help you protect tenant data and secure sensitive documents focusing on sensitivity labels and data loss prevention

Deployment methodologies and common issues

Microsoft Purview Information Protection

Discover, classify, and protect sensitive information wherever it lives or travels

Know your data

Understand your data landscape and identify sensitive data across your environment

Protect your data

Apply flexible protections actions including encryption, access restrictions and visual markings

Prevent Data Loss

Detect risky behaviour and prevent accidental oversharing of sensitive information

Govern your data

Automatically retain, delete, and store data and records in a compliant manner

chess® Making it Easy to work **Securely, Anywhere, Anytime**

Know your data

A user will interact with multiple services during their working day

Some services will be used to store and process sensitive information.

Tenant information

- PII, Names, addresses, contact information
- Medical details
- Crime information
- Benefits

Employee Data

- Employment record
- Pay information

Confidential Business Information

- Finance
- Board
- Legal

IT Data

- Systems information
- Passwords

Know your data

A user will interact with multiple services during their working day

Some services will be used to store and process sensitive information.

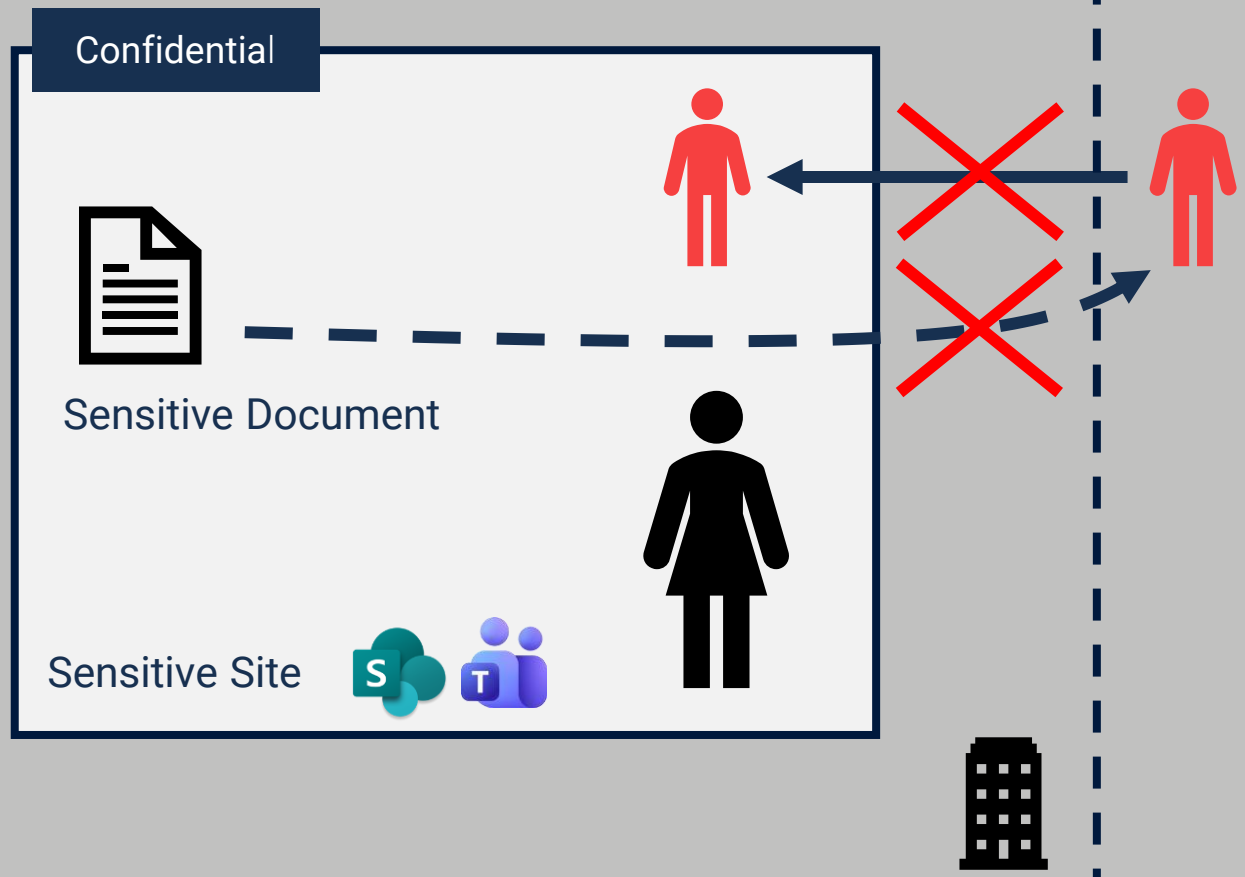
Chat	Email	Storage	Storage	Generative Prompt
Collaboration	Attachments	Sharing	Sharing	
Guest Access	Calendar Invites	Guest Access	Download	
Meetings		Download		

Protect your data - Sensitivity Labels

Use Information Protection sensitivity labels to classify and control access to sensitive data

Groups and Sites	Files	Emails	Meetings
Privacy and access control for: Teams Microsoft 365 groups SharePoint Sites Loop Workspaces	Data classification Marking Encryption Access control	Data classification Marking Access control Message Encryption	Protect Teams meetings and chats

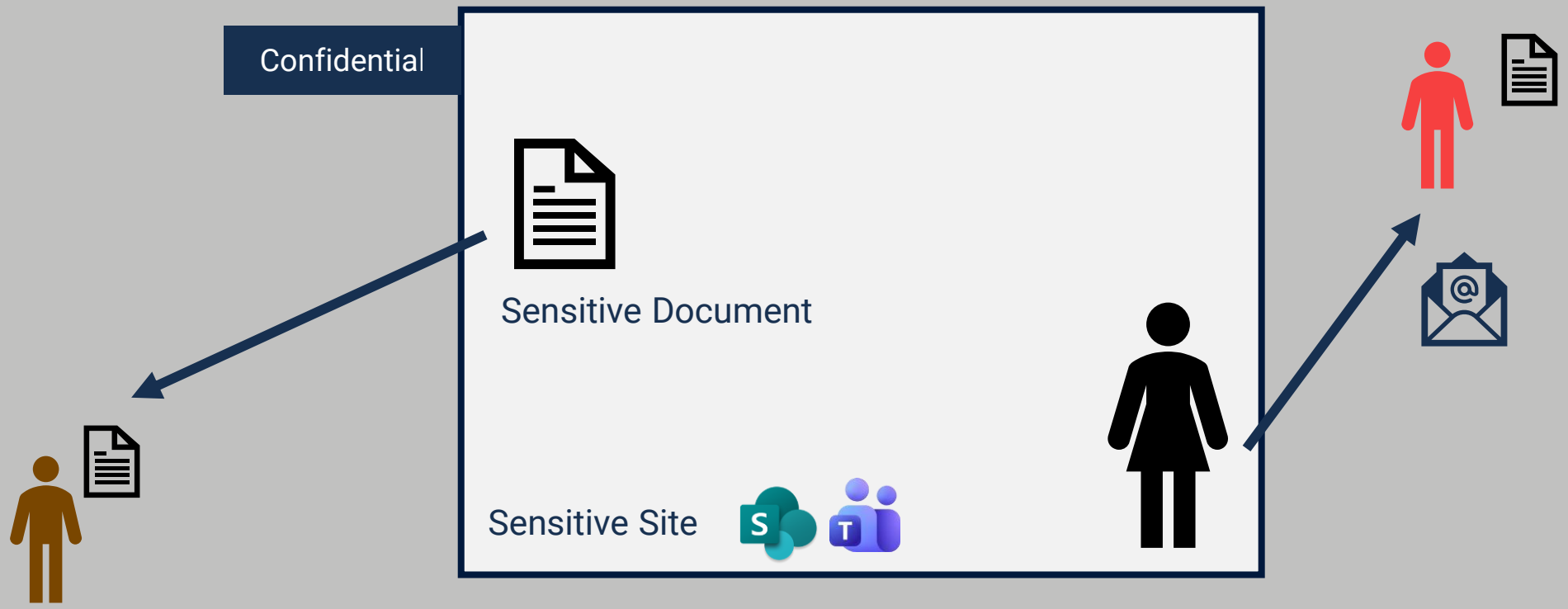
Sensitivity Labels – Groups and Sites



- Allow or block guest access
- Define the SharePoint Sharing Policy
- Enforce site or Teams Privacy (private/public)
- Private Team Discoverability
- Control use of Teams shared channels
- Unmanaged device access

Sensitivity Labels – Files and Emails

How do we protect content outside of the container?



Sensitivity Label - Demo

Sensitivity Labels – Files & Emails Recap

Embed security into files and emails

- Apply an organisational classification scheme
- Encrypt and permission documents
- Create preset permissions or allow user defined
- Apply in office applications or SharePoint
- Label data at rest
- Mark document with header/footer/watermark
- Encrypt Email encryption/do not forward
- PDF support
- Auto labelling to assist users
- Respected by Copilot

Prevent Data Loss - DLP

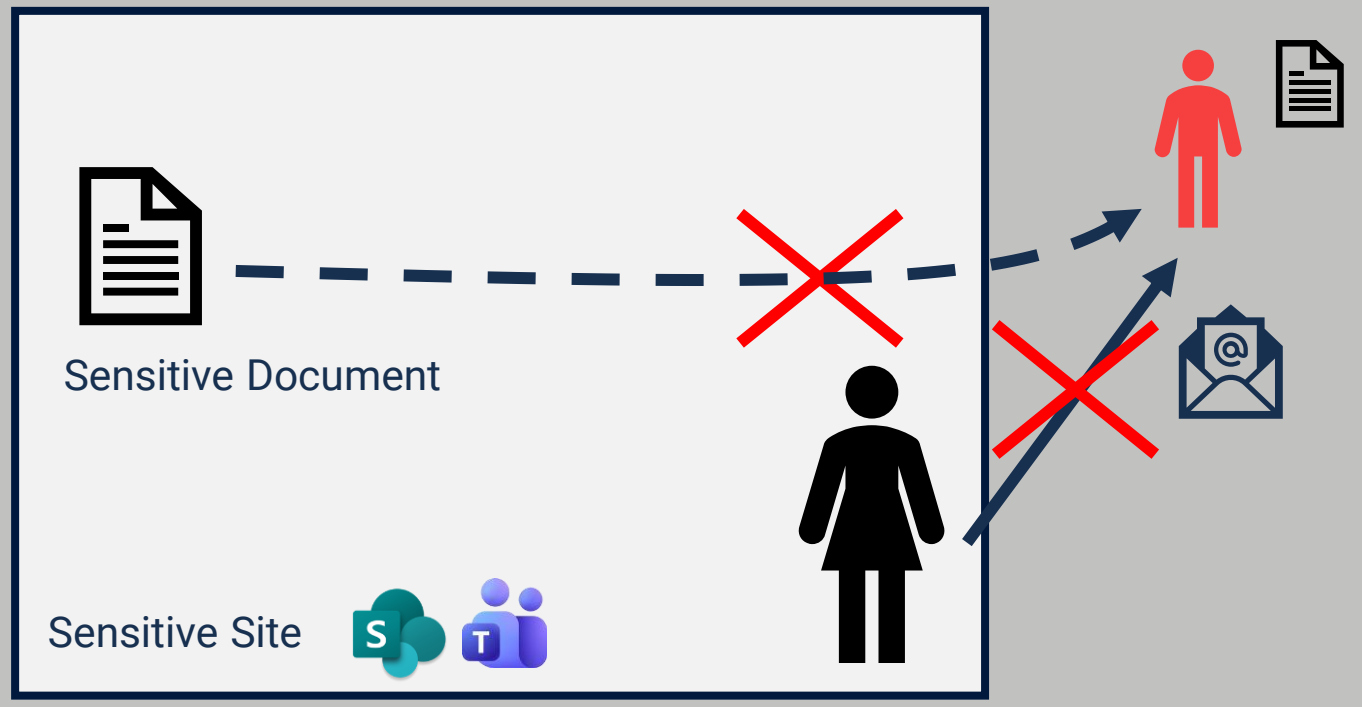
Prevent sharing of sensitive information

- Email
- SharePoint Online
- OneDrive for Business
- Teams chat and channel messages
- Microsoft 365 Copilot and Copilot Chat
- Microsoft Edge for Business
- Devices
- On-premises repositories

Data Loss Prevention - Demonstration

How does DLP protect content?

- Detect
- Apply Action
- Notify
- Alert and Report



DLP Demo

Deployment – Considerations and Issues

Information Protection is a complex project

- Significant Undertaking – Multi-month project
- Impact to working practices must be understood
- Incorrect project stakeholders/ownership
- User adoption and training is key
- Short term design can lead to future issues
- Don’t do too much too fast
- Organisation not invested.

Deployment - Approaches

Multiple deployment models

Crawl – Walk - Run

Traditional method that takes an iterative approach to deployment following the information protection framework.

Secure by default

Use this deployment model to help rapidly implement a secure by default configuration with Microsoft Purview Information Protection, Data Loss Prevention, and Insider Risk Management.

Lightweight guide to mitigate data leakage

Use this deployment model to enable core data security capabilities with minimal configuration, focusing on essential steps to get started quickly

New – September 2025

Next Steps

Find our more!

To learn more about the Information Protection, explore new features, and discover the next steps for deployment, simply tick the “Request for Follow-Up” box on the survey.