

# Developing Digital Skills



Co-funded by  
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Coordinator:

**MMC** Mediterranean  
Management Centre

Partners:



ПРИВРЕДНА КОМОРА РЕПУБЛИКЕ СРПСКЕ  
ПОДРУЧНА ПРИВРЕДНА  
КОМОРА БАЊА ЛУКА

**DIMITRA**  
educational organization



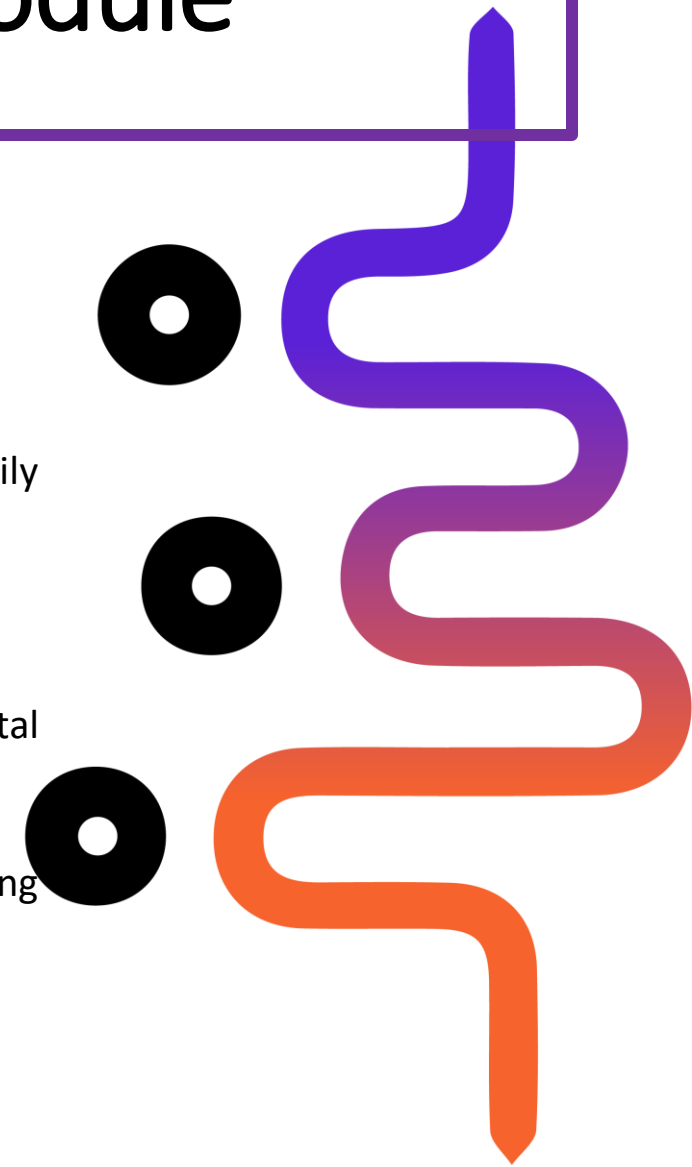
**CETEO**  
**Asnor**  
Associazione Nazionale Orientatori



# Objectives of the module

## In terms of knowledge:

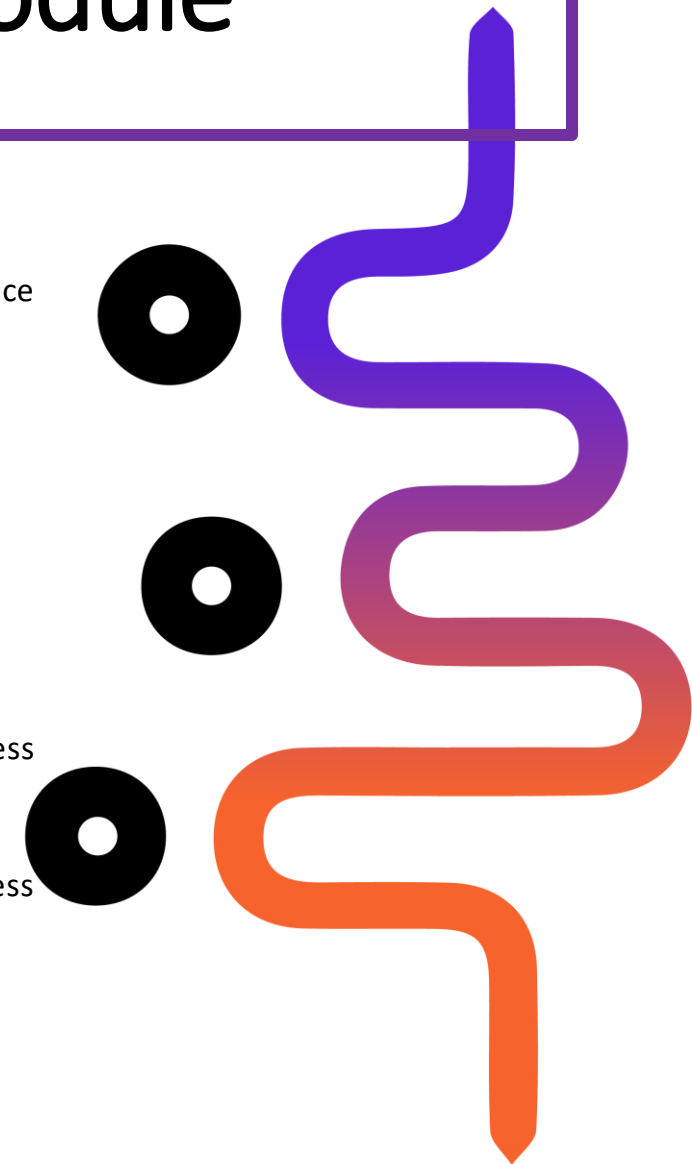
- Analyze common digital safety risks in workplace environments and explain their potential organisational impact.
- Interpret and apply core GDPR principles in relation to routine workplace data handling situations.
- Differentiate and justify structured approaches to managing digital information and data in daily professional tasks.
- Identify and compare appropriate digital tools and AI applications based on specific workplace needs.
- Explain and justify professional standards for digital communication and collaboration in digital workspaces.
- Describe and sequence structured troubleshooting procedures for common digital problems, including criteria for escalation.
- Explain the rationale for continuous digital upskilling in rapidly evolving workplace environments.



# Objectives of the module

## In terms of skills:

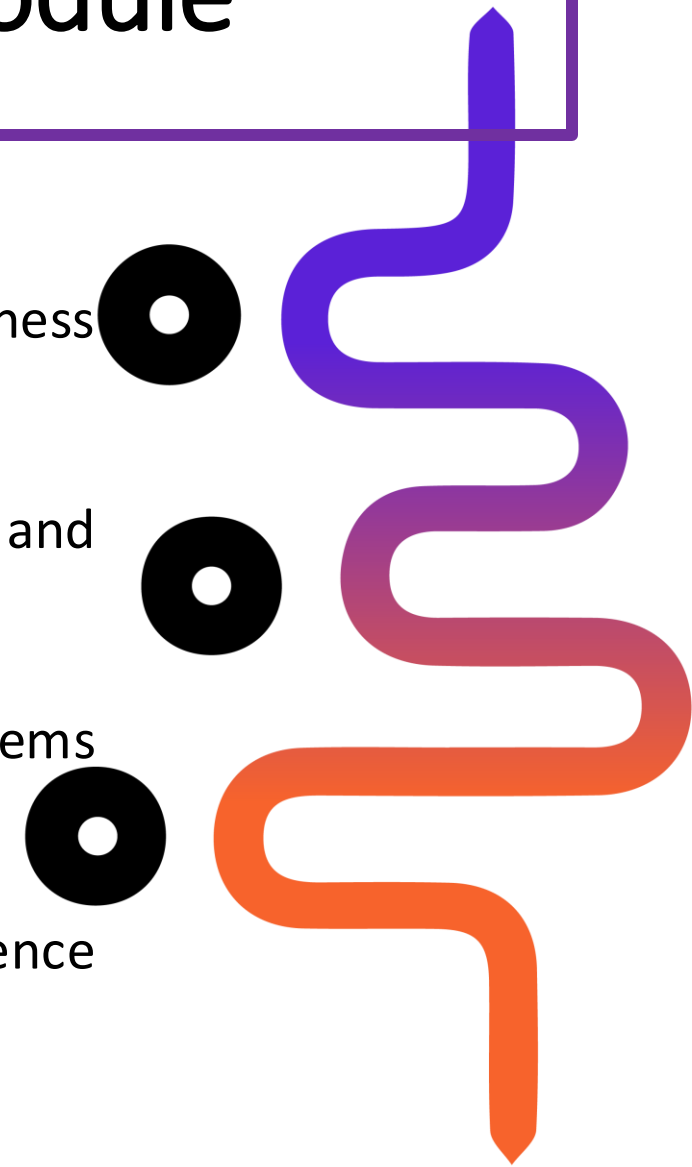
- Implement appropriate digital protection measures to reduce cybersecurity and data protection risks in routine workplace activities.
- Critically evaluate digital information sources and content to determine reliability and suitability for professional use.
- Organise, categorise and manage digital files and information using structured systems that enhance operational efficiency.
- Select and apply appropriate digital productivity tools to produce standard workplace deliverables autonomously.
- Use AI-based tools responsibly and strategically, ensuring protection of sensitive data and critical evaluation of AI outputs.
- Collaborate autonomously through digital technologies, managing sharing settings, co-editing workflows and access permissions appropriately.
- Diagnose and resolve common technical issues using structured troubleshooting logic and document the resolution process where required.
- Assess personal digital competence levels and design a structured improvement plan to address identified gaps.



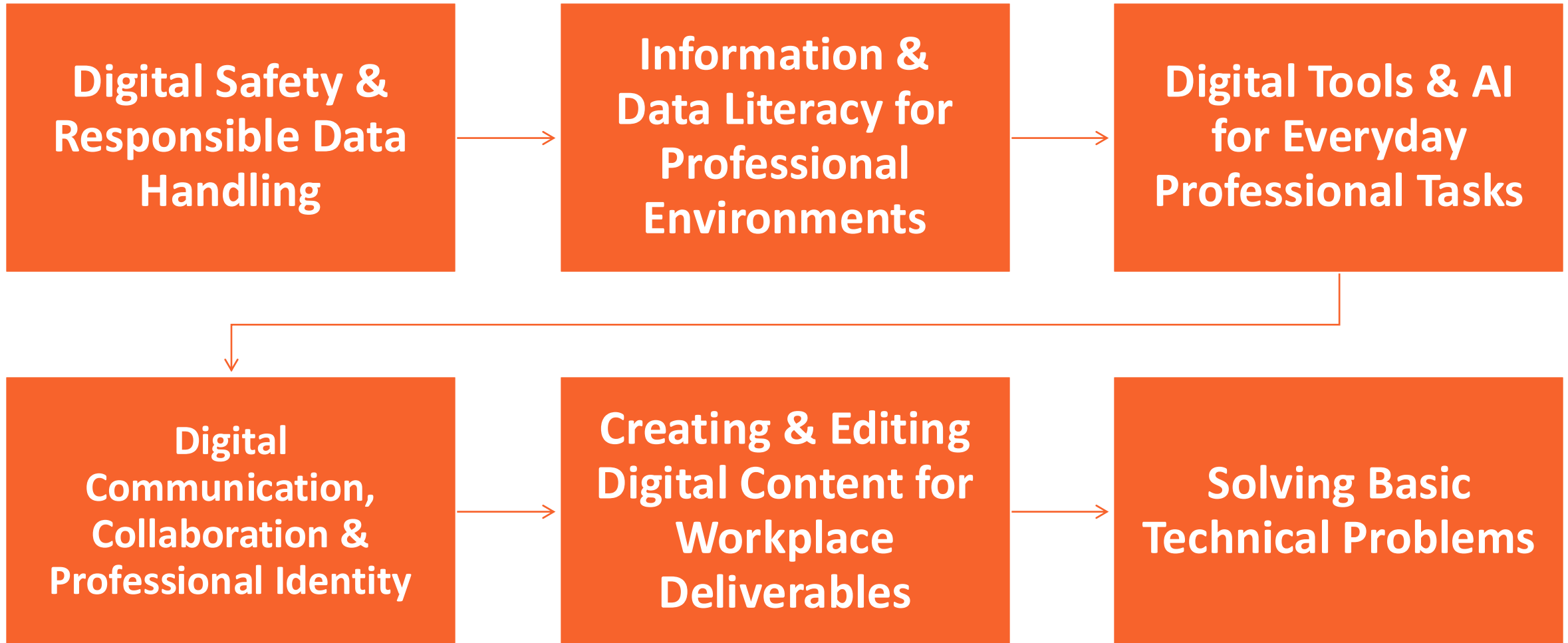
# Objectives of the module

## In terms of attitudes:

- Demonstrate commitment to data protection, cybersecurity awareness and ethical digital conduct in professional environments.
- Exhibit responsibility and professionalism in digital communication and collaborative digital practices.
- Display proactive behaviour in identifying and addressing digital problems within workplace contexts.
- Adopt a continuous learning mindset towards digital competence development in response to technological change.

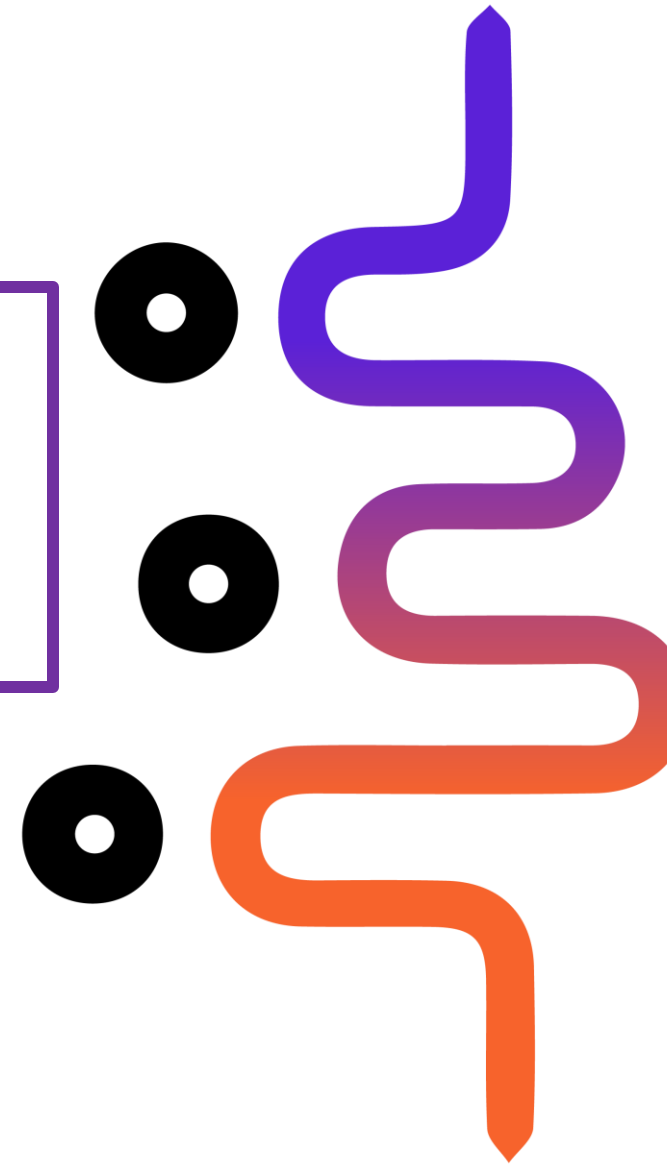


# Module routemap



# Digital Safety & Responsible Data Handling

## Unit 1



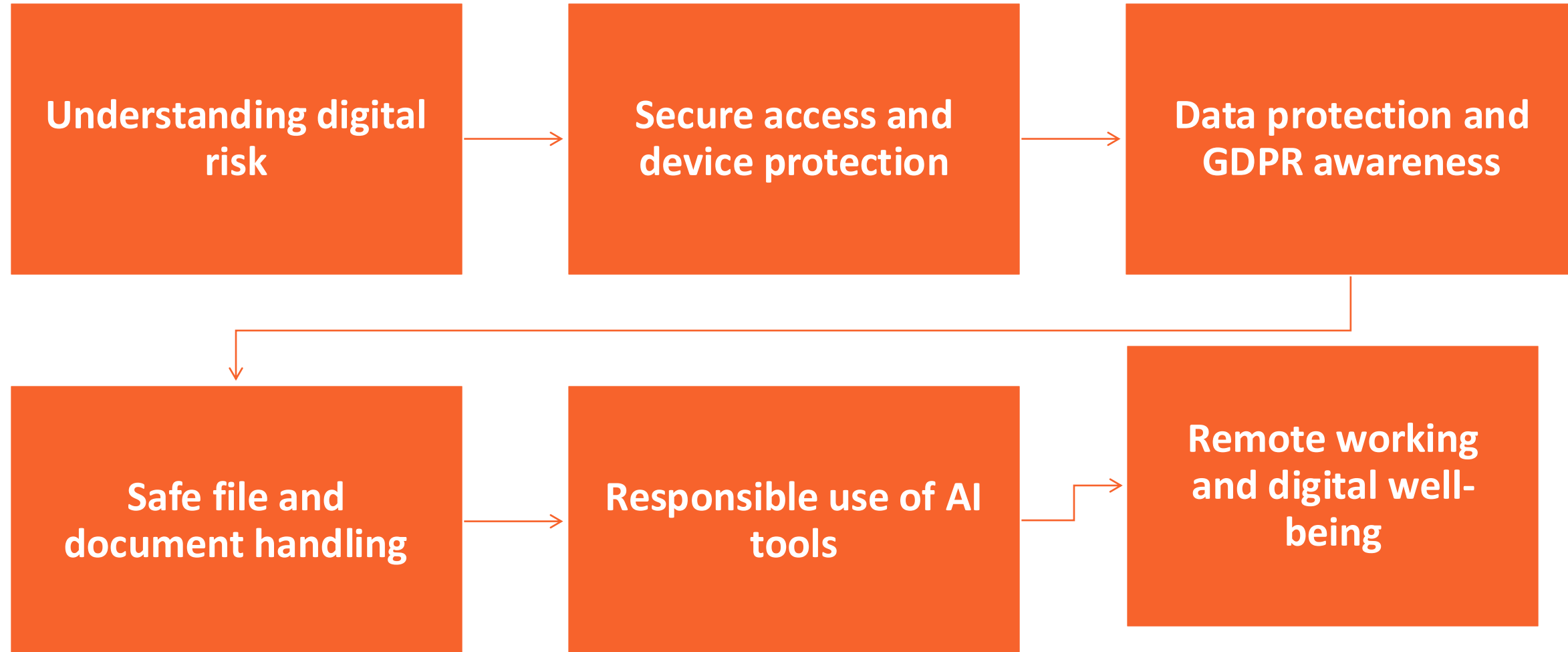
# Why this unit matters

This unit introduces the principles and practices that support safe, responsible and effective participation in digital work environments. It focuses on risk awareness, responsible handling of information and informed judgement in routine professional activities.

In contemporary workplaces, digital safety is a basic professional requirement. Unsafe digital behaviour can lead to data exposure, interrupted operations, damaged trust, legal or compliance issues and reduced quality of work. Responsible digital conduct is therefore part of effective performance, not a secondary concern.



# Unit routemap



# TOPIC 1 – UNDERSTANDING DIGITAL RISK



# What is digital safety?

**Digital safety** refers to the set of behaviours, controls and decisions that help individuals and organisations use digital technologies without unnecessarily exposing data, systems, privacy, well-being or operational continuity to risk.

It includes:

- protection of devices and accounts
- careful handling of information
- safe communication
- awareness of digital environments
- responsible judgement



# Digital safety in workplace reality

**Digital safety** is not only relevant in exceptional incidents.

It appears in ordinary activities such as:

- checking email
- sharing files
- storing documents
- using online platforms
- logging into systems
- working remotely
- using AI-supported tools

Routine tasks can create significant risk when completed without verification or care.

# What is digital risk?

A **digital risk** is any condition, event or behaviour that may negatively affect:

- information confidentiality
- data integrity
- system availability
- privacy
- trust
- quality of work



**Digital risks** can arise from **both technical vulnerabilities and human behaviour**.

Example: *Sending a file to the wrong recipient. A typical case where the risk is associated with human error, which could lead to exposure of confidential data.*

**Digital risk = any threat to data, systems, privacy or workflow caused by digital activity.**

# Types of Digital Risks in the Workplace

**Digital risks** in the workplace typically fall into several categories, each representing a different kind of threat to the integrity of data, devices and systems. Most threats fall into predictable categories, which helps us recognise and prevent them.

**Common workplace threats** include:

- **Phishing:** deceptive messages designed to obtain information or trigger unsafe action.
- **Malware:** harmful software that disrupts, steals or damages.
- **Social engineering:** manipulation of people to gain access or compliance.
- **Weak authentication:** poor password and login practices.
- **Unsafe sharing:** uncontrolled access to files and data.

[ENISA's cyber hygiene guidance](#) centres on exactly these kinds of everyday prevention practices. Recognising immediately the category helps determine the correct response.

# Phishing

**Phishing** is a form of cyber attack in which attackers impersonate legitimate organizations (or by disguising as a trustworthy entity) to steal sensitive information such as login credentials, credit card details or company secrets.

**Phishing attacks** often use **social engineering tactics** to deceive the recipient into believing the message is from a trusted source, causing them to act without proper verification.

Example:

*An employee receives an email from what appears to be the bank, claiming that their account has been compromised and they need to click a link to update their details. This link leads to a fake website designed to steal login information.*



The main risk is **identity theft** or **financial fraud**. Phishing can also provide attackers with access to internal systems, leading to larger data breaches or malware infections.

# Identifying phishing

Indicators of a suspicious message include:

- **unusual sender address** → may imitate a trusted organisation but contains small inconsistencies (e.g. extra letters or domains)
- **request outside normal procedure** → bypasses established workflows or approval processes
- **unexpected attachment or link** → may redirect to malicious websites or install malware
- **urgent or threatening tone** → reduces critical thinking by pressuring the user to act quickly without checking
- **grammatical inconsistency or unusual formatting**
- **request for confidential data or codes** → violates organisational security policies

A message may still look professional and yet remain unsafe.

## Practice rule:

Do not click on links or open attachments from unknown or suspicious emails. Always verify the sender's email address and never act immediately on urgent digital requests without verification.

# Case Study: Analysing a Phishing Email

## Scenario: Example of a Suspicious Email

**Subject:** Urgent: Security Issue Detected on Your Workstation

**From:** Margaret Doe, IT Supervisor [m.doe@ourcompany.com](mailto:m.doe@ourcompany.com)

**To:** John Sample

**Email Content:**

John,

The IT security team has detected unusual activity on your workstation during late hours. We believe your device may be affected by a recently identified security issue.

Please review the attached log files and confirm whether these actions were performed by you.

If not, please click the link below to update your antivirus software immediately:

 [Update Security Software](#)

Let me know once completed.

Margaret  
IT Supervisor

## Analysis of the Email

### 1. Personalisation

The message uses the employee's name ("John") → increases trust

### 2. Fake but realistic sender

Domain looks correct but slightly altered → ourcompany.com instead of ourcompany.com

### 3. Authority

Message appears to come from IT department → increases compliance

### 4. Fear trigger

"Your device may be affected" → creates urgency and concern

### 5. Low-risk engagement

"Review attached log files" → builds trust before main action

### 6. High-risk action

"Click the link to update software" → actual attack vector (malware or credential theft)

# Malware

**Malware** (malicious software) refers to software created to compromise a device, system or dataset. It may arrive through unsafe downloads, malicious attachments, fake updates or compromised websites.

Example: *Opening an infected attachment.*

**Possible consequences include:**

- loss of files
- reduced system performance
- unauthorized access
- service interruption
- wider spread across systems

## Practical rules:

- Ensure that antivirus software is installed and updated on all devices.
- Do not download software or updates from untrusted sources and only use reputable platforms for work-related applications.



# Key Types of Malware

## 1. Ransomware

- encrypts organisational data and demands payment (often in cryptocurrency)
- targets availability of data

## 2. Spyware

- silently monitors user activity (keystrokes, screen, credentials)
- targets confidentiality

## 3. Trojan Horses

- disguised as legitimate tools (e.g. PDF converter, update file)
- installs malicious code when executed

# Social engineering: the human dimension of cyber risk

**Social engineering** refers to manipulating people instead of systems. It involves manipulating individuals into divulging confidential information, often by exploiting psychological manipulation rather than technical means.

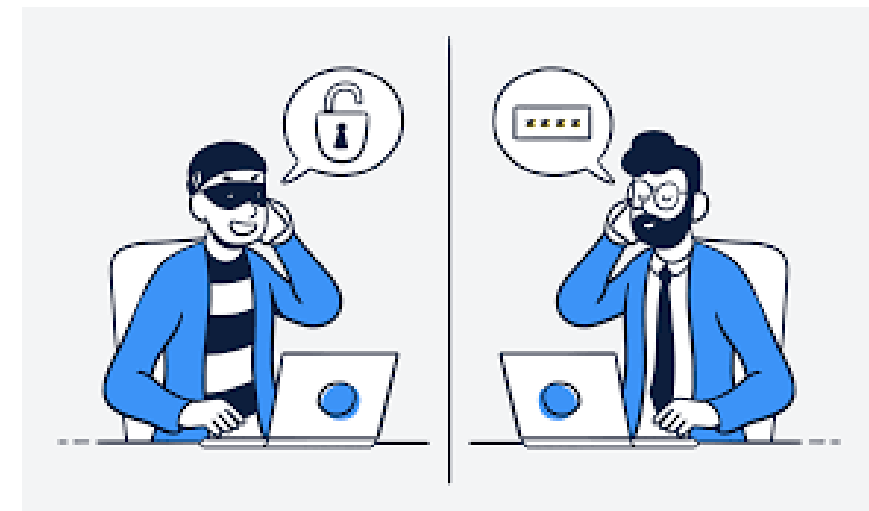
**Attackers** may pretend to be legitimate employees, vendors, or customers to gain trust and convince the victim to disclose sensitive data or provide access to systems.

## Example:

*An attacker calls an employee claiming to be from the HR department and convinces them to share the company's internal login details or access credentials.*

## Practice rule:

Verify all unsolicited requests for sensitive information by contacting the requesting party through official communication channels. Be cautious when receiving unsolicited calls or emails that request login credentials or access to company systems.



# Why routine work is often vulnerable?

Employees often carry multiple responsibilities, work under time pressure and rely on relatively informal communication practices. This can increase the likelihood of unsafe shortcuts, insufficient checking and inconsistent control over data and access.

Many digital incidents do not happen because users know nothing. They happen because users are:

- rushed
- distracted
- multitasking
- overconfident
- following habit rather than judgement

Risk therefore often emerges from ordinary workflow conditions.

**Digital safety depends heavily on behaviour.**

# Case Study: The Cost of a Click

This case shows how **social engineering** can lead to a technical security breach through a simple user action.

## Scenario

An employee receives an email titled:

### “Tax Invoice – Urgent Review Required”

- Appears to be from a legitimate vendor
- Professional and work-related
- Requests opening an attached invoice

The request seems routine and safe.

## Why It Works (Social Engineering)

- **Trust** → familiar business context (invoice)
- **Relevance** → part of daily tasks
- **Urgency** → encourages immediate action
- **Low perceived risk** → opening files feels normal

### Attack Progression, Result & Impact

After the employee opens the attachment, malicious code is executed, infecting the system and allowing the malware to spread across the internal network. As a result, organisational files are encrypted through a ransomware attack, making all client data inaccessible and disrupting business operations. The organisation faces significant consequences, including recovery costs exceeding €50,000, operational downtime and loss of productivity. The most critical impact, however, is the loss of client trust, which may have long-term or irreversible effects.

## TOPIC 2 - SECURE ACCESS & DEVICE PROTECTION



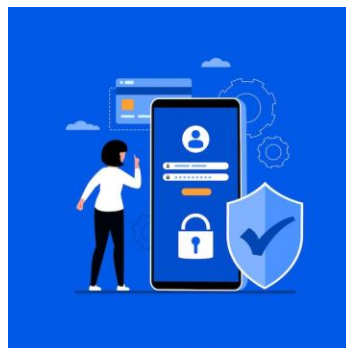
# Why authentication matters

**Authentication** is the process of verifying the identity of a user, device, or entity before granting access to a system or data.

**Effective authentication is the first line of defense** against unauthorized access. This includes using passwords, biometrics, smart cards and other methods to ensure the right person is accessing systems.

## Example:

*When logging into a secure portal, users must enter a password and confirm their identity using a fingerprint scanner or a second authentication factor, such as a mobile code.*



# Passwords as a first line of defense

**Passwords** remain one of the most common access controls. Their effectiveness depends not only on complexity but also on length, uniqueness and user behaviour.

Brute-force attacks can crack 8-character passwords in minutes. Poor password practice weakens even well-designed systems.

|                    |                                        |                              |
|--------------------|----------------------------------------|------------------------------|
| Choose a password: | <input type="password" value="....."/> | Password strength: Too short |
|                    | Minimum of 8 characters in length.     |                              |
| Choose a password: | <input type="password" value="....."/> | Password strength: Weak      |
|                    | Minimum of 8 characters in length.     |                              |
| Choose a password: | <input type="password" value="....."/> | Password strength: Fair      |
|                    | Minimum of 8 characters in length.     |                              |
| Choose a password: | <input type="password" value="....."/> | Password strength: Good      |
|                    | Minimum of 8 characters in length.     |                              |
| Choose a password: | <input type="password" value="....."/> | Password strength: Strong    |
|                    | Minimum of 8 characters in length.     |                              |

From google.com

# Principles of stronger passwords

## 1. Length is Top Priority

- Use at least 16 characters.
- Longer passwords are harder to guess via brute-force.

## 2. Uniqueness

- Never reuse passwords across sites.
- A breach on one site shouldn't compromise others.

## 3. Complexity/Randomness

- Mix character types: letters, numbers, and special characters.
- Example: 6MonkeysRLooking^.

## 4. Use Passphrases

- Combine 4–7 unrelated random words (e.g., "BlueSkyCoffee\*2024").
- Long and easier to remember.

## 5. Avoid Personal Info

- Do not use names, birthdays, dictionary words, or common sequences like "123456" or "password123".

Passwords should be long, unique, and not based on personal info. Store them securely, and don't reuse across accounts

# Unsafe Password Practices

## 1. Password Reuse

- Using the same password across multiple platforms.
- One breach compromises all accounts.

## 2. Weak/Simple Passwords

- Predictable words, birthdays, pet names, or short sequences.
- Easily cracked by automated tools.

## 3. Storing Passwords Insecurely

- Writing passwords on sticky notes, storing in plain text files, or using unencrypted browser auto-fill.

## 4. Sharing Credentials

- Sharing passwords via unencrypted email, text, or with others.

## 6. Not Updating After Breaches

- Continuing to use a password after it has been exposed in a data breach.

### Consequences of Poor Password Security

**Credential Stuffing:** Hackers gain access to other services using stolen credentials.

**Identity Theft:** Unauthorized access to personal information.

**Financial Loss:** Direct theft or fraudulent purchases from bank accounts.

# Common Password Habits & Creation Mistakes

## 5 Common Password Habit Mistakes

- Reusing passwords
- Physically storing passwords
- Not changing passwords after a breach
- Storing passwords in a browser
- Insecurely sharing passwords

## 6 Common Password Creation Mistakes

- Including familial names
- Including personal info
- Including personal preferences
- Using simple sequences like “56789”
- Using predictable characters or dictionary words
- Creating short, simple passwords

# Multi-factor authentication (MFA)

**MFA** strengthens access protection by requiring more than one form of verification. It is known as “The Gold Standard of Protection”.

It typically combines:

- something the user knows (e.g. Password/PIN)
- something the user has (e.g. Smartphone/Security Key)
- or something the user is (e.g. Biometrics, Fingerprint/FaceID)

It does not remove all risk, but it significantly reduces risk if credentials are exposed. Even if one factor is compromised, access is still protected.

Example: *Using a password combined with a fingerprint scan or a code sent via SMS.*

## MULTI-FACTOR AUTHENTICATION



# How MFA Works (Step-by-Step Process)

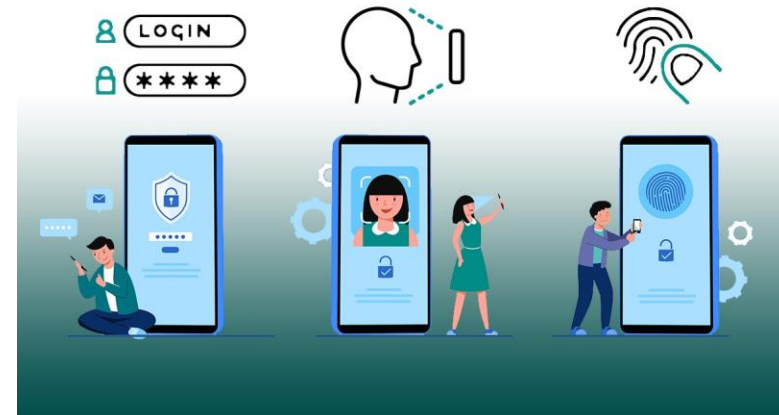
When accessing a secure system, authentication takes place in multiple stages:

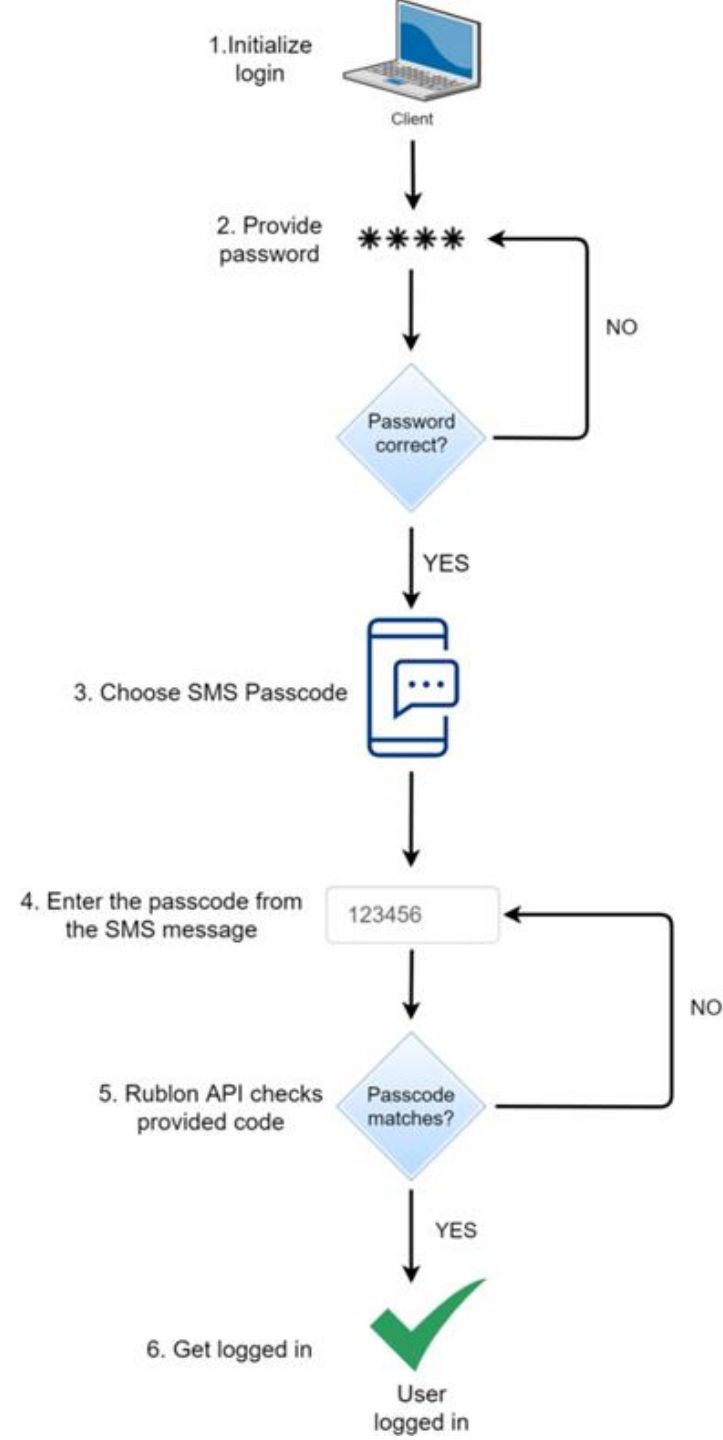
1. The user enters their **username and password**
2. The system verifies the credentials
3. A **second authentication request** is triggered
4. The user receives a **one-time passcode (OTP)** on their mobile device or authentication app
5. The user enters the verification code
6. Access is granted **only if both authentication factors are correct**

## Risk (Without MFA)

Without multi-factor authentication:

- stolen or weak passwords can lead to **full system access**
- phishing attacks can easily compromise user accounts
- attackers may gain access to **sensitive organisational data and systems**





# Responsible device security

**Device security** involves the practice of protecting endpoints like laptops, smartphones and desktops from unauthorized access, theft or malware.

As **devices are the main points of entry to data and systems**, ensuring their security is paramount. This includes using firewalls, encryption, anti-virus software, and secure configurations.

## **Secure device use includes:**

- locking screens when away
- using approved software
- avoiding unknown downloads and USB devices
- protecting devices during travel
- keeping systems and applications updated



Example: *Locking your computer when leaving your desk, ensuring that sensitive data is encrypted, and updating security software regularly.*

# Why Updates matter

Updates often:

- correct known vulnerabilities
- improve system reliability
- reduce compatibility issues
- strengthen protection against known threats

**Keeping software updated ensures protection** against known vulnerabilities and keeps systems secure from external threats.

Example: *Regularly updating operating systems, antivirus programs, and browsers to patch security holes.*

Failing to apply patches may leave systems open to exploitation by malware or hackers.

## Practical rule:

Enable automatic updates for critical software, and prioritize updates for operating systems and security software.

# Key Types of Updates

| Type                                 | Purpose                                                           | Example                                                                  |
|--------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Patch</b>                         | Fixes specific issues affecting system performance or security    | <i>Fixing a calculation error in accounting software</i>                 |
| <b>Hotfix</b>                        | Urgent fix for critical issues outside the regular update cycle   | <i>Immediate fix for a system crash during daily operations</i>          |
| <b>Security Update</b>               | Addresses vulnerabilities that could be exploited by attackers    | <i>Fixing a weakness that allows unauthorized access to company data</i> |
| <b>Critical Update</b>               | Resolves major system errors affecting functionality              | <i>Fixing issues that prevent access to core business systems</i>        |
| <b>Cumulative Update</b>             | Combines multiple previous fixes and improvements into one update | <i>Installing one update instead of multiple smaller ones</i>            |
| <b>Service Pack</b>                  | Bundle of patches, fixes and updates for easier deployment        | <i>Company-wide system update across all employee devices</i>            |
| <b>Feature Update / Feature Pack</b> | Introduces new features and improves system functionality         | <i>New tools for collaboration or workflow efficiency</i>                |
| <b>Upgrade</b>                       | Major version change of software or operating system              | <i>Moving from Windows 10 to Windows 11</i>                              |

# TOPIC 3 – DATA PROTECTION & GDPR AWARENESS



# What counts as data in workplace practice?

Workplace data includes:

- names and contact details
- customer records
- employee information
- schedules
- internal reports
- contracts
- financial documents
- communication records



Not all data has the same sensitivity, but all data requires appropriate handling.

# Personal data

**Personal data** refers to any information that can identify an individual, either directly or indirectly. This includes common identifiers such as names, contact details, identification numbers and even online identifiers.

## Examples:

- *name*
- *email address*
- *phone number*
- *identification details*



# GDPR awareness for employees

**GDPR (General Data Protection Regulation)** is the European Union regulation that protects personal data and sets guidelines for processing it.

At employee level, GDPR awareness does not require legal expertise. It requires disciplined professional behaviour, such as:

- accessing only what is necessary
- using data only for legitimate work purposes
- sharing through approved channels
- avoiding careless exposure
- reporting mistakes promptly

The European Commission's data protection guidance is the most reliable high-level public source for this.

[The European Commission's Data Protection Guidance](#)



# The 7 Core Principles of GDPR

## 1. Lawfulness, Fairness and Transparency

Data must be collected and used in a lawful and transparent way (e.g. Inform customers why their data is collected and how it will be used).

## 2. Purpose Limitation

Data must only be used for the specific purpose it was collected for (e.g. Customer data collected for billing cannot be used for marketing without consent).

## 3. Data Minimisation

Only the necessary data should be collected (e.g. do not request unnecessary personal details in forms).

## 4. Accuracy

Personal data must be accurate and kept up to date (e.g. regularly update customer contact details).

## 5. Storage Limitation

Data should not be kept longer than necessary (e.g. delete outdated employee or client records).

## 6. Integrity and Confidentiality (Security)

Data must be protected against unauthorized access or loss (e.g. use secure systems, passwords and restricted access).

## 7. Accountability

Organisations must be able to demonstrate compliance with GDPR (e.g. maintain records of how data is handled and protected).

# Why responsible data handling matters

## Poor data handling can affect:

- the rights and interests of individuals
- organisational credibility
- customer trust
- quality of internal operations
- legal and compliance obligations

Data protection is therefore **ethical, operational and regulatory** at the same time.

Non-compliance with GDPR may lead to significant fines and reputational damage.

# Common workplace data-handling mistakes

**Data handling mistakes** refer to errors made while managing, storing or sharing data.

Examples include:

- sending files to the wrong recipient
- oversharing access in folders
- storing documents in unapproved locations
- copying unnecessary recipients into emails
- exposing printed or visible data
- sharing more data than the task requires

These errors can lead to privacy violations, data leaks, and damage to the organisation's reputation.

# What to do after a data-handling mistake

Even with the best precautions, data-handling mistakes can happen. The critical point is to handle mistakes promptly and responsibly to mitigate potential damage.

A **responsible response** usually includes:

1. assess the situation
2. do not conceal the incident
3. notify the appropriate person or function
4. follow internal procedure
5. limit further exposure where possible
6. learn from the event

# TOPIC 4 – SECURE FILE & DOCUMENT HANDLING



# Why file organisation matters

**File organisation** refers to the systematic method of storing, naming, and accessing digital files to ensure that they are easily retrieved, protected and managed securely.

**Proper file organisation minimizes risks** such as accidental data exposure, miscommunication and inefficient retrieval. It ensures that sensitive information is only accessible to authorized individuals and helps maintain operational efficiency.

Example: *Using clear folder structures and naming conventions to organize documents by project or department, rather than storing files in arbitrary or general folders.*

Clear naming, structured folders, controlled versions and approved storage reduce:

- confusion
- duplication
- accidental sharing
- outdated use of documents
- unnecessary exposure



File organisation is therefore both a **productivity issue** and a **safety issue**.

# Key Principles for Digital File Organization

## 1. Create a Logical Structure

- Build a hierarchy based on your workflow (e.g., by client, project, or date).
- Keep subfolders shallow (3–4 levels) to avoid excessive clicking.

## 2. Consistent Naming Convention

- Develop a standard naming system (e.g., YYYY-MM-DD\_DocumentName\_Version).
- Use camel case or underscores instead of spaces.
- Avoid using special characters.

## 3. Version Control

- Avoid names like final\_v2\_updated.doc. Use \_v01, \_v02 for sequential revisions.
- Consider using software-tracked changes.

## 4. Archive/Clean Up Regularly

- Move completed projects to an archive folder to reduce clutter.

## Best Practices Recap

- **Go Shallow:** Limit subfolders to 3–4 levels.
- **Use Descriptive Names:** Think ahead—what will you search for later?
- **Act Immediately:** Save files directly to their final location, not to your desktop.
- **Archive Consistently:** Regularly move old files to an archive folder or cloud storage.

# Principles of safer file sharing

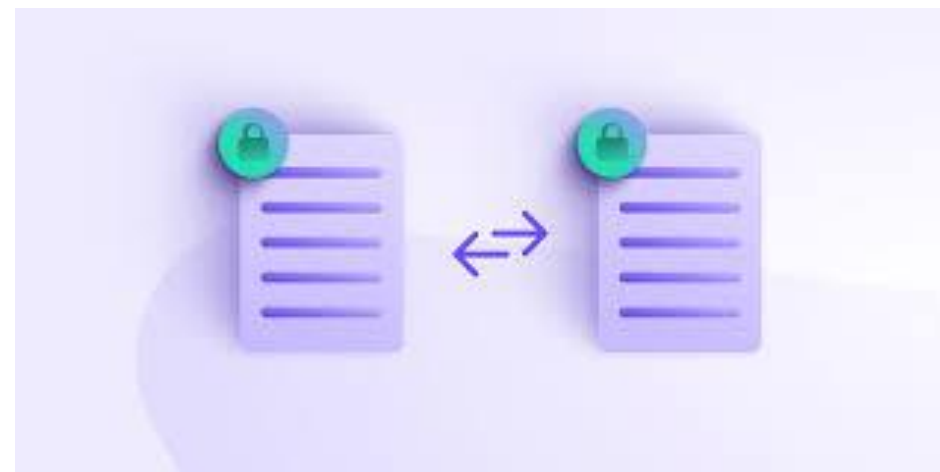
**File sharing** refers to the process of transferring files from one location to another, either within an organization or externally, while ensuring the files are shared securely and appropriately.

**File sharing becomes risky** when improper settings are used, or when files are shared with unauthorized people. To protect both the integrity of the data and its confidentiality, it's crucial to follow a structured process that includes access control, encryption and sharing via approved platforms.

Example: *Sending a file to an external partner through an encrypted email service, instead of using an unsecured public link.*

Before sharing a file, consider:

- who actually needs access
- what permission level is necessary
- whether the file is the correct version
- whether the platform used is approved
- whether access should be time-limited



# Maintaining Control Over Documents in Digital Environments

Unlike traditional file sharing (e.g. email attachments), controlled access systems ensure that the file **remains within a managed environment** rather than being duplicated across multiple devices.

Modern platforms such as OneDrive, Google Drive and SharePoint provide mechanisms to control:

- **access** (who can open the file)
- **visibility** (who can see it exists)
- **usage** (view, comment, edit, download)

This transforms file sharing from **distribution to controlled access**.

Example: *Instead of emailing a financial report, an employee shares a restricted access link with a client.*

- Access is limited to specific users
- Downloading is disabled
- Access can be revoked at any time

**Secure file sharing is not about sending files, it is about maintaining control over data throughout its lifecycle.**

## Risks

- loss of control once files are sent
- uncontrolled forwarding or duplication
- storage of sensitive data in unsecured locations
- inability to track access or usage

## Correct Practice

- Share links instead of attachments
- Use organisation-approved platforms only
- Restrict access to specific users
- Regularly review and revoke access when no longer needed

# Protecting Sensitive Documents

**Sensitive document protection** involves securing both the visible content and the hidden data (metadata) within a file to prevent unintended information disclosure.

Documents often contain **hidden information** that is not visible during normal viewing, including author details, editing history, tracked changes, internal comments, file paths or system references.

- This metadata can reveal confidential organisational information if not removed.
- Example: *An employee shares a Word document externally without cleaning it. The recipient can see the internal discussions, previous edits and names of employees or clients.*

Security is not only about protecting what is visible, it also requires controlling hidden and background information.

## Risks

- exposure of internal strategy or communication
- disclosure of confidential client information
- reputational damage and GDPR compliance risks

## Correct Practice

- Use document encryption for sensitive files
- Apply password protection when necessary
- Remove metadata using tools such as “Inspect Document”
- Share passwords via a separate communication channel

## TOPIC 5 – RESPONSIBLE USE OF AI TOOLS



# Artificial Intelligence: Productivity Tool or Risk Factor?

**AI tools** are software that use machine learning and artificial intelligence to process data, automate tasks and generate insights.

**AI can boost productivity**, but it can also create risks, especially when dealing with personal or sensitive data. Using AI responsibly means ensuring data privacy, security, and compliance with the law.

AI tools may help with:

- summarising information,
- structuring text,
- generating first drafts,
- supporting idea organisation.

## Risk

Every prompt entered into a public AI system is a potential data transfer to an external system

### Example:

*If you're using AI to summarize customer feedback, ensure that no personally identifiable information (PII) is included in the dataset.*

**AI is not just a tool it is a data-processing environment.**

# Risks of Using AI Tools

## Risk 1: Unauthorized Use of Personal Data

Sharing or using personal information without proper consent or security measures.

## Risk 2: Misuse of AI Insights

AI can generate insights, but if used poorly, these insights could lead to biased or unfair decisions.

## Risk 3: Non-Compliance with Data Protection Laws

Violating laws like GDPR by mishandling personal or sensitive data.

Example: *Using AI to analyze customer feedback but including sensitive data like phone numbers or email addresses.*

### AI should be used to:

- support decision-making
- improve productivity

### NOT to:

- replace professional judgement
- process sensitive data without control

# Best Practices for Responsible AI Use

## **Practice 1: Anonymize Data**

Always make sure to anonymize data before inputting it into AI tools.

## **Practice 2: Avoid Sharing Sensitive Data**

Only share personal data with AI tools if it's absolutely necessary and ensure it's explicitly approved.

## **Practice 3: Choose Compliant AI Tools**

Use AI tools that are compliant with data protection laws (e.g., GDPR).

Example:

*For customer sentiment analysis, remove or anonymize any personally identifiable data (e.g., names, emails) before submitting it.*

# AI Hallucinations and Uncontrolled Use of AI Tools

**AI hallucination** is when AI generates incorrect or misleading information presented as accurate.

**Shadow AI** is the use of unauthorized AI tools outside organisational control.

AI tools can introduce two major risks:

## 1. Unverified Outputs (Hallucinations)

AI may appear reliable or provides incomplete or incorrect information or generates content without valid sources.

## 2. Uncontrolled Use (Shadow AI)

Employees may use personal AI tools to save time, automate tasks or process work-related data.

**Both risks affect decision-making and data protection.**

### Risks

- incorrect business or technical decisions
- professional errors and liability
- loss of data control
- absence of audit trail
- exposure of organisational or personal data
- use of data in external AI training models

### Correct Practice

- always verify AI-generated content
- cross-check with trusted and official sources
- never rely blindly on AI outputs
- use only approved (enterprise) AI tools
- avoid personal AI accounts for work tasks

# When Convenience Leads to Data Exposure

## Scenario

An employee uses a public AI tool to analyse customer feedback and includes real data such as names, emails and transaction details. The action seems efficient, but introduces hidden risks.

**What Happens** → The data is processed outside the organisation, resulting in loss of control and exposure of sensitive personal information.

## Why This Is a Problem

- personal data shared without proper basis
- violation of confidentiality and data minimisation
- creates a direct GDPR compliance risk

## Impact

- data breach
- legal and financial consequences
- loss of customer trust

### Correct Practice

- never input personal data into public AI tools
- anonymize data before use
- use only approved AI solutions

**Using AI with real data without control is equivalent to sharing it with a third party**

# TOPIC 6 – REMOTE WORKING & DIGITAL WELL-BEING



# The Workplace is Everywhere

**Remote work** extends the organisational environment beyond the office to homes, public spaces and mobile settings.

When working remotely, the organisation loses direct control over:

- networks
- devices
- physical environment

**This increases exposure to security risks.**

Digital safety depends not only on systems, but also on **where and how work is performed.**

# Remote working risks

## Understanding the Exposure

**Remote working risks** refer to the security challenges and potential vulnerabilities that arise when working outside a traditional office setting, often on personal devices or unsecured networks.

Remote work may **expose learners to:**

- public or insecure Wi-Fi networks
- visible screens in public spaces
- shared or personal devices
- overheard conversations
- unattended equipment
- distracting environments

### Risks

- data interception
- unauthorized access
- accidental exposure of sensitive information

Working remotely therefore requires deliberate protective behaviour.

Example: *Working from a café and accessing company files on open Wi-Fi.*

# Safer remote-working behaviour

## Safer practice includes:

- using safer networks where possible
- protecting screen visibility
- locking devices when away
- separating work and personal use
- handling files carefully outside the main workplace
- avoiding sensitive tasks in exposed environments when possible

### From Home Network to Device Protection

- change default router passwords
- enable strong Wi-Fi encryption (WPA2/WPA3)
- use separate networks for work devices
- activate VPN when working remotely

**Remote work requires deliberate and conscious behaviour, not automatic routines.**

# Digital well-being as part of digital safety

**Digital well-being** refers to the sustainable and healthy use of digital technologies, ensuring that individuals do not suffer from digital overload, stress, or burnout due to excessive use of digital tools.

Excessive use of digital technologies, especially for work, can lead to digital fatigue, which reduces productivity, increases errors, and leads to poor decision-making.

Example:

*Constantly checking emails or notifications throughout the day, leading to distracted work and mental fatigue.*

# How digital overload affects safety

Digital overload may lead to:

- rushed decisions
- poor checking before sending
- careless clicking
- weak concentration
- constant task-switching
- more frequent avoidable mistakes

Digital well-being is therefore not only a personal comfort issue; it is also a **security issue**.

# Practical Digital Well-being Habits

## **1. Take regular short breaks**

→ reduces fatigue and improves attention

## **2. Manage notifications**

→ limit interruptions to avoid constant task-switching

## **3. Use focused work blocks**

→ dedicate uninterrupted time to complex or sensitive tasks

## **4. Slow down before sending or clicking**

→ verify recipients, links and attachments before action

## **5. Apply extra care with sensitive data**

→ double-check content, access and context before sharing

**A focused user is a safer user.**

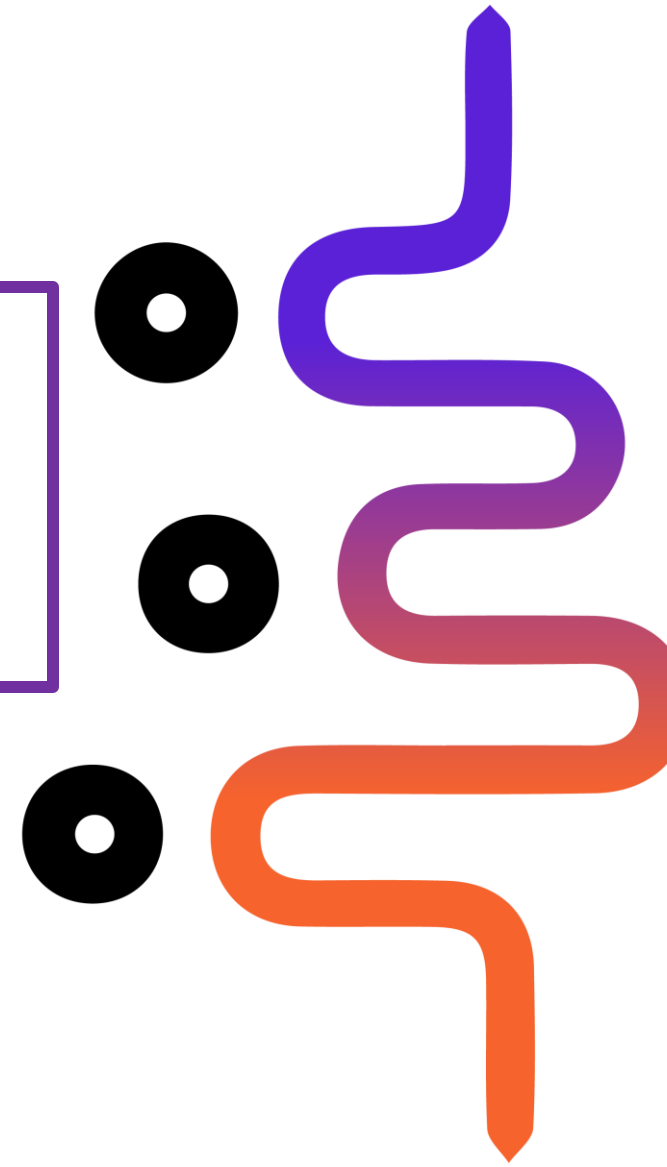
Digital safety depends not only on tools, but on attention, discipline and self-management.

# References & Further Reading

- European Commission (2024) *EU Data Protection Rules (GDPR)*. Available at: [https://commission.europa.eu/law/law-topic/data-protection\\_en](https://commission.europa.eu/law/law-topic/data-protection_en) (Accessed: 26 March 2026)
- OECD (2023) *OECD AI Principles Overview*. Available at: <https://oecd.ai/en/ai-principles> (Accessed: 27 March 2026)
- European Commission (2024) *Ethics Guidelines for Trustworthy AI*. Available at: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (Accessed: 27 March 2026)
- OECD (2022) *Productivity and Digitalisation in the Workplace*. Available at: <https://www.oecd.org/digital> (Accessed: 26 March 2026)
- ENISA (European Union Agency for Cybersecurity) (2023) *Cyber Hygiene: Guidelines for SMEs and Organisations*. Available at: <https://www.enisa.europa.eu/topics/cyber-hygiene> (Accessed: 24 March 2026)
- National Cyber Security Centre (NCSC) (2023) *Multi-factor authentication (MFA): how to set up and use it*. Available at: <https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services> (Accessed: 25 March 2026)

# Information & Data Literacy for Professional Environments

## UNIT 2



# Unit Structure



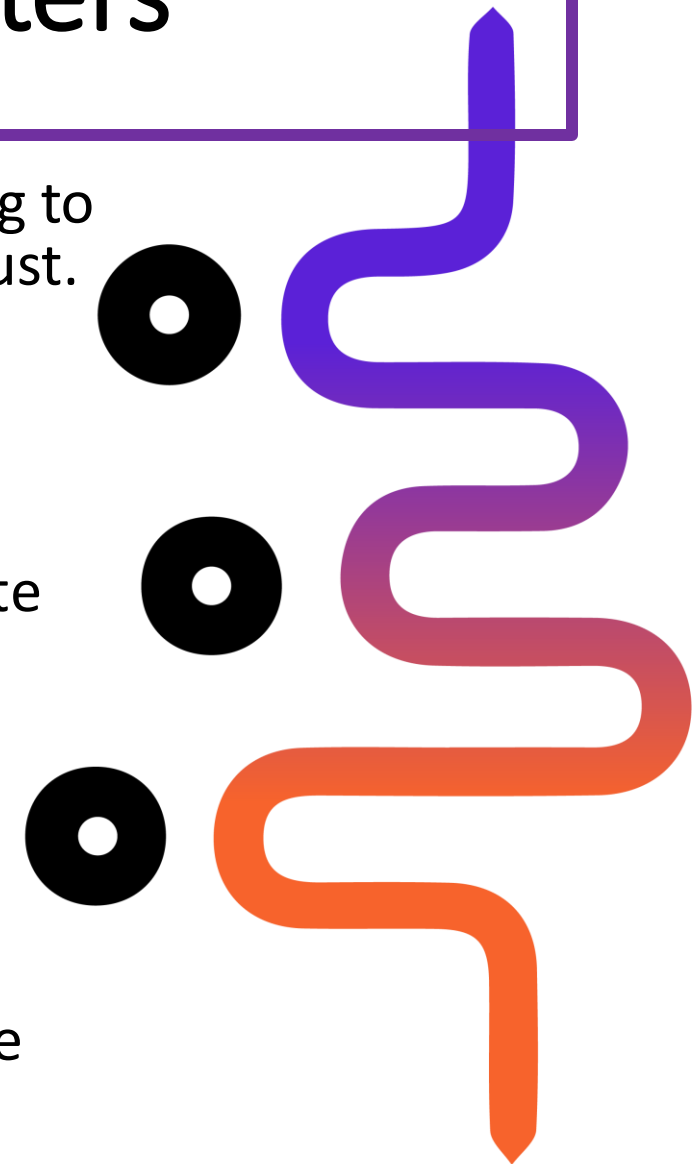
# Why This Unit Matters

In contemporary workplaces, information is not simply “something to access”. It is a working resource that shapes action, quality and trust.

Poor information and data practices can lead to:

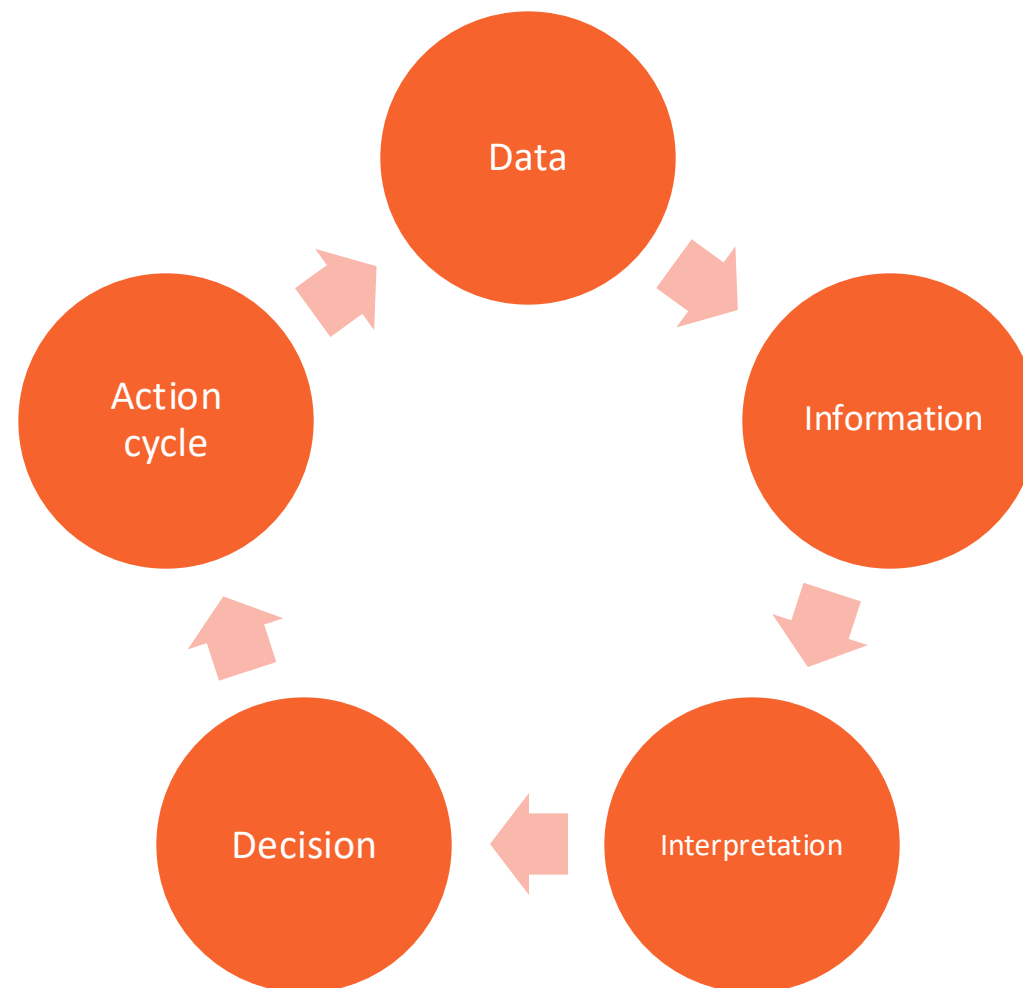
- **Operational problems** such as delays, duplication, confusion, wrong versions, inconsistent reporting.
- **Financial consequences** such as poor supplier choices, inaccurate calculations, inefficient use of time and resources.
- **Compliance and ethical risks** such as misuse of sensitive information, weak control over shared files, poor traceability.
- **Reputational damage** such as reduced trust from managers, colleagues, clients or external partners.

In micro-enterprises these risks are amplified because one mistake often affects multiple processes at the same time.



# TOPIC 1 - UNDERSTANDING DATA AND INFORMATION

# From Information to Decision Lifecycle



# Information Literacy as a Professional Asset

**Information literacy** is the ability to **find, evaluate, organize and use information** effectively and ethically. It's a skill that applies to any field and is critical for making informed decisions, solving problems and advancing knowledge in the workplace.

## Key Components of Information Literacy:

- **Finding Information:** Knowing where to search, which databases or platforms to use and how to filter out irrelevant information.
- **Evaluating Information:** Assessing the credibility, accuracy and relevance of the information.
- **Organizing Information:** Creating systems for managing information that ensure accessibility and traceability.
- **Using Information:** Applying information to solve problems, support decision-making, or create new knowledge.

Being information literate means going beyond simply accessing data. It's about developing the ability to **critically engage** with information to use it effectively in the workplace. In modern workplaces, information is not neutral or passive. It is a **core working resource** that directly affects decisions (what actions are taken and why), operations (how work is organised and executed) and outcomes (quality, efficiency and results).

# Data vs Information vs Knowledge

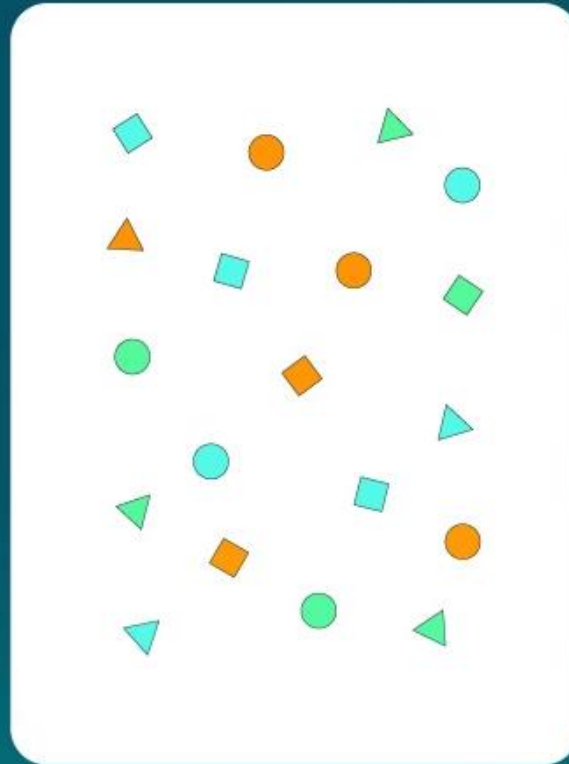
- **Data:** Raw facts and figures that have little meaning on their own.  
Example: "25, 10, 35" are just numbers without context.
- **Information:** Data that is organized or processed to have meaning.  
Example: A report showing sales numbers for the last quarter provides context to the numbers, such as trends or insights.
- **Knowledge:** Information that is interpreted, understood and applied in decision-making or action.  
Example: A manager using the sales report to forecast next quarter's sales and adjust the marketing strategy accordingly.

Understanding the difference between these concepts is crucial to making informed decisions.

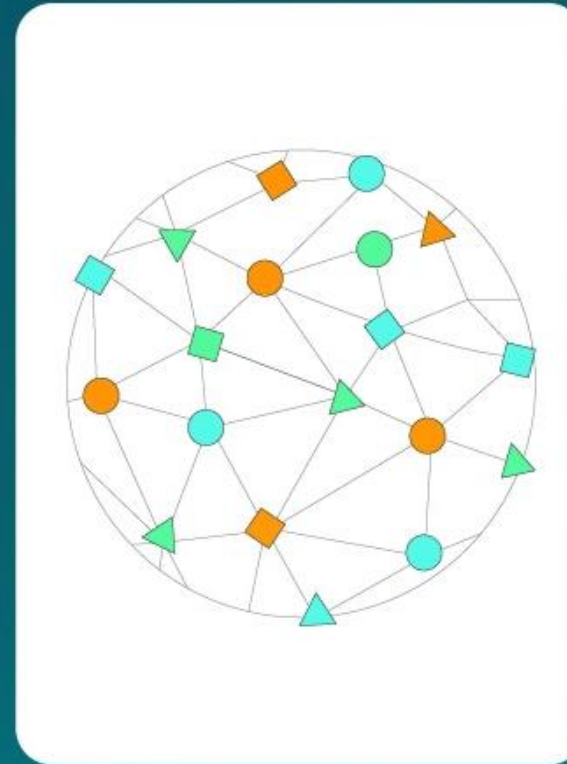
The key to using information effectively is understanding its context and transforming it into actionable knowledge. Data alone is often useless without the appropriate interpretation.

# Data vs Information vs Knowledge

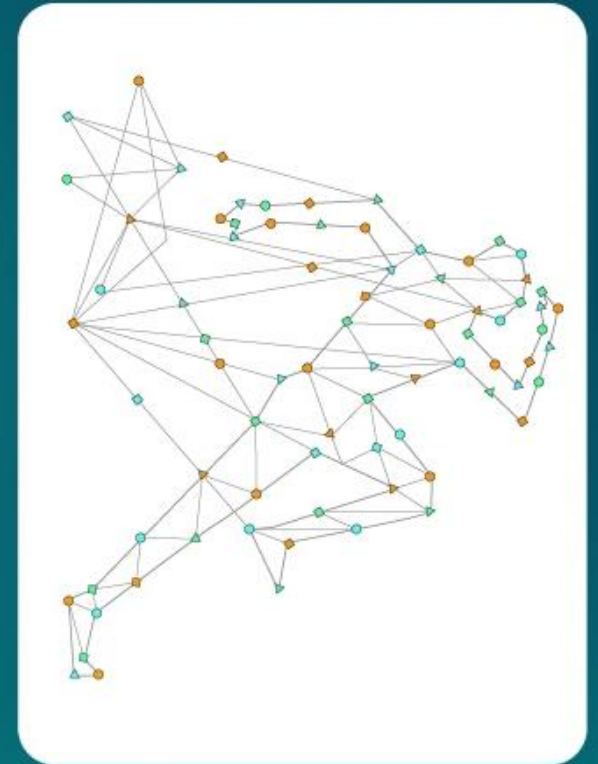
**Data**



**Information**



**Knowledge**



# Structured vs Unstructured Data

**Structured Data:** Data that is organized into rows and columns, often found in databases or spreadsheets. It is easy to enter, search, filter, store, query and analyze.

Example: *A customer database with fields for customer name, phone number and email.*

**Unstructured Data:** Data that doesn't follow a predefined format. It can be more challenging to organize and analyze.

Example: *Emails, social media posts, text files, PDFs and multimedia files.*

Unstructured data can often contain valuable insights, but it requires proper processing to unlock its full potential. Structured data is easier to process and analyze, while unstructured data often holds valuable insights that require additional work to interpret and organize.

Professionals need to understand how to manage both structured and unstructured data, as they both play crucial roles in decision-making and analysis.

A comprehensive guide comparing structured and unstructured data. It explores the key differences in format, storage, and analysis, while explaining how modern Lakehouse architectures manage all three types to drive business intelligence and AI.

[Structured vs Unstructured Data](#)

## Unstructured Data



Vs

## Structured Data



# Workplace Reality

Employers increasingly expect:

- Critical thinking
- Ability to evaluate information
- Adaptability in handling different data sources
- Learning by doing and problem solving

In a typical workplace, especially in SMEs, employees often juggle multiple tasks and are required to make quick decisions. This environment often results in **limited access to perfect data** and **incomplete information**.

*Example: A sales manager may need to analyze market trends, customer feedback and internal performance data, but may only have access to fragmented pieces of information.*

**Informed decisions** often require piecing together various types of data and information from different sources. Understanding the nature of the information at hand and organizing it systematically is key to avoiding errors and inefficiencies.

# Risks of Poor Information Handling

## Consequences of Poor Information Management:

- **Wrong Decisions:** Using incorrect or unreliable information can lead to poor business decisions.
- **Operational Delays:** Mismanaged data can cause delays in processes or missed deadlines.
- **Compliance Risks:** Using outdated or incorrect information can result in failing to meet regulatory requirements.
- **Financial Losses:** Wrong financial data can lead to bad investments or missed opportunities.

*Example: An employee could make incorrect financial forecasts based on outdated sales data, leading to poor budgeting decisions and financial losses.*

Failure to handle information effectively creates a **domino effect** that can lead to operational inefficiency and significant business risks.

Explore more about the risks of poor data management in this [IBM Guide to Data Management](#)

# What This Means for You

To work effectively with information, you must:

- Understand what information **is and what is not**
- Recognise when information is **incomplete or unreliable**
- Organise data in a way that supports **action and traceability**
- Apply information with **judgement and responsibility**

Employers are emphasizing **meta-competencies** such as adaptability, initiative and critical thinking over narrowly defined technical skills. Information management is no longer just about gathering data but about using it effectively.

Developing a **holistic approach to information** that includes not just data management skills, but also critical thinking and adaptability, is essential for meeting modern workplace demands.

# TOPIC 2 – SEARCHING AND EVALUATING INFORMATION

# Types of Workplace Information Needs

In every professional environment, employees need to find and process information to complete tasks, solve problems or make decisions. These needs can vary across industries and roles.

Key types of information needs include:

- **Operational Information:** Information required to run daily operations efficiently (e.g., supplier details, pricing, inventory levels).
- **Regulatory Information:** Information related to laws, regulations, compliance requirements (e.g., health and safety guidelines, GDPR policies).
- **Technical Information:** Information related to specific tools, machinery, or software (e.g., user manuals, troubleshooting guides).
- **Customer-Related Information:** Information on customer needs, feedback, preferences, and history (e.g., CRM systems, customer service inquiries).

The type of information needed can differ widely based on the task at hand and understanding what type of information is required will help you target your search more effectively.

# Professional Sources

## What Makes a Source Professional?

- **Credibility:** Reliable sources are written by experts or recognized organizations in the field. For example, articles from academic journals, government publications, or reputable institutions.
- **Authority:** Sources from recognized authors or publishers, such as industry leaders, professors or professional associations.
- **Accuracy:** Information that can be verified through multiple sources, ensuring it is factual and trustworthy.
- **Relevance:** Information should be up-to-date and relevant to the specific task or question you are researching.

## Examples of Professional Sources:

- Academic journals (e.g. ResearchGate, Academia.edu)
- Industry reports (e.g., from big companies like Deloitte)
- Government publications (e.g., EU regulations, official guidelines)

Relying on professional sources ensures that the information you use is **accurate, reliable, and valid**, which is crucial for making informed decisions in the workplace.

# Understanding Different Types of Information Sources

In professional environments, information is produced and accessed through different types of sources, each with different levels of reliability, authority and purpose:

- **Official / Institutional Sources** (e.g. European Commission, legislation, regulatory bodies, internal policies) → High reliability, formal validation, legally relevant
- **Professional / Industry Sources** (e.g. technical documentation, supplier data, industry reports) → Practical, specialised, but may include commercial bias
- **Internal Organisational Sources** (e.g. company files, reports, databases, previous work) → Context-specific, operationally relevant, but may be outdated or inconsistent
- **Open Web Sources** (e.g. websites, blogs, forums, articles) → Easy access, variable quality, often not validated
- **AI-Generated Content** (e.g. ChatGPT, Gemini, copilots) → Fast and structured, but requires verification and critical judgement

**The value of information depends heavily on where it comes from.**

# Searching Strategies

**Effective Searching** is essential for retrieving relevant and accurate information. The key strategies include:

- **Use Precise Keywords:** When searching online or in databases, using specific, targeted keywords will return more relevant results.
- **Apply Filters:** Most search engines and databases allow you to filter results based on various factors such as date, author, or type of resource (e.g., scholarly articles, reports).
- **Use Multiple Sources:** Don't rely on just one source. Cross-referencing from different sources increases accuracy and credibility.

An effective search strategy requires more than just typing a few words into a search engine.

Define clearly the question before searching.

Good searching starts with a clear problem definition, not with a tool.

# Risks in Searching

## Potential Pitfalls of Searching for Information:

- **Outdated Information:** Using old data or research can lead to decisions based on obsolete facts.
- **Bias in Sources:** Some sources may present information with a particular bias (e.g., commercial websites promoting their own products).
- **Incomplete Information:** A source may omit important context or leave out key facts, leading to misunderstandings or errors.

## Common Risks:

- Using **unverified online sources** like blogs or personal websites.
- Relying on **social media** or **user-generated content** that may not be reliable.

To make well-informed decisions, it's crucial to be aware of the **risks** involved in searching for and using information. Evaluating the credibility of sources is an essential part of the information-gathering process.

# Tools for Searching Information: Traditional Search Engines

## Traditional Search Engines:

**Google** is the most widely used search engine globally. It uses a combination of **algorithms** to rank web pages based on their relevance and quality.

### How Google Works:

1. **Crawling:** Google uses bots to explore the internet and index web pages.
2. **Indexing:** Pages are categorized based on keywords, links and page content.
3. **Ranking:** Based on algorithms, Google ranks pages by relevance and authority, factoring in criteria like keywords, backlinks, site security and user engagement.

### Search Tips:

- Use **specific keywords** for better results.
- Apply **filters** (e.g., date range) to narrow down results.
- Use **Google Scholar** for academic resources.
- Use **Google News** for up-to-date information.

#### Top results are not always:

- the most accurate
- the most reliable

#### So you should:

- check multiple results
- look beyond the first page
- identify source credibility

#### **Risk**

- Assuming: “first result = best result”
- Search engines optimize for relevance and engagement, not always for truth or reliability.

# The New Trend: AI-powered Tools for Searching Information

AI-powered tools such as ChatGPT and Google Gemini are changing the way we interact with search engines.

Instead of simply returning a list of web links, these tools use advanced **Natural Language Processing (NLP)** to provide direct answers summarise complex topics quickly understand natural language queries or even engage in conversational searches.

## How AI Tools Work:

- **Input Understanding:** The user inputs a question or query, and the AI analyzes it for context and intent.
- **Data Retrieval:** The AI pulls from vast amounts of **pre-trained knowledge** and **data** (books, websites, reports, etc.).
- **Response Generation:** It generates a response based on patterns, facts and its training, offering a clear, direct answer rather than links.
- Example: Asking ChatGPT "What are the main differences between structured and unstructured data?" results in a direct, well-structured answer, rather than a list of links to articles.

## Why AI Search is a Game Changer:

- **Efficiency:** Provides direct answers, saving time for users who need immediate information.
- **Contextual Understanding:** Can interpret more complex, multi-step queries and provide nuanced answers.
- **Personalized Interaction:** These tools can remember past conversations (to an extent) and refine responses over time.

# Evaluating Information: Core Criteria

Before using information, evaluate:

- **Accuracy**  
Is the information correct and free of errors? Can it be verified through other trusted sources?
- **Relevance**  
Does the information directly address the question or issue at hand? Is it timely and useful for your decision-making process?
- **Authority**  
Who is the author or source? Do they have the necessary expertise or credentials to speak on the subject?
- **Timeliness**  
Is the information current? In fast-changing industries, using outdated information can lead to poor decisions.
- **Purpose**  
What is the intent behind the information? Is it objective, or is it trying to persuade or sell you something?

Ignoring evaluation leads to:

- misuse of information
- incorrect decisions

Always apply at least **2–3 criteria before use**. Evaluation is a **decision filter**, not an optional step.

[UNC Chapel Hill – Evaluating Information Guide](#) provides a structured and widely used framework for assessing the quality, credibility and usefulness of information sources, applicable in both academic and workplace environments.

# Identifying Unreliable Information

## Signs of Unreliable Information:

- **No Source or Citation:** Lack of a clear source means the information cannot be verified, making it suspect.
- **Bias or Emotional Language:** Information that uses overly emotional or biased language to push an agenda should be treated with caution.
- **Unclear or Misleading Author:** If the author's credentials are vague or not directly related to the topic, be skeptical.
- **Exaggerated Claims:** Statements that promise extreme or too-good-to-be-true outcomes without proper evidence.
- **Inconsistent or Contradictory Information:** If the information contradicts established facts or expert consensus, it should be carefully scrutinized.

Being able to identify **red flags** helps you avoid misinformation and focus on trustworthy sources.

# Evaluating AI-Generated Information

AI tools, such as ChatGPT or Google Gemini, are designed to answer questions and provide information quickly, but **they don't verify facts** in real-time.

AI can generate content that **appears accurate** but may be based on outdated, incomplete or biased data.

## Limitations of AI in Information Evaluation:

- **No real-time validation:** AI doesn't access live data to ensure the current relevance of the information.
- **Bias in training data:** AI is trained on vast datasets, some of which may include biased or inaccurate information.
- **Lack of context:** AI may not fully understand nuanced, complex situations that require human interpretation.

## Best Practice for AI-Generated Information Use:

- Always **cross-check** AI-generated information with other credible sources.
- Understand that **AI tools** are there to assist but not to replace **critical evaluation**.
- Use AI responsibly to **support decision-making**, but not as the sole source of truth.

The responsibility for accuracy remains with the human user, not the tool.

# What Do You Do When Sources Conflict?

You find:

- Source A says one thing
- Source B says another

In that occasion you should:

- check source authority
- compare multiple references
- prioritise official or validated data
- delay decision if necessary



Choosing the easiest or fastest answer is not the correct practice.

Professional judgement is tested when information is **uncertain or conflicting**.

# Risk Impact of Poor Information Evaluation

## Risk Implications of Poor Evaluation:

- **Legal Risks:** Using outdated compliance information can result in **finances** or **lawsuits**.
- **Operational Risks:** Misunderstanding technical documentation can lead to equipment failures or delays in production.
- **Financial Risks:** Poor market analysis can result in bad investment decisions or missed opportunities.
- **Reputational Risks:** Relying on biased or false information can harm the reputation of the company and lead to customer distrust.

Evaluating the quality and reliability of information **mitigates risks** and ensures that decisions are made in line with professional standards and industry regulations.

**Incorrect supplier data → wrong contract → financial loss**

# Professional Workflow for Evaluating Information

A structured approach:

- **Verify Information:** Cross-check facts and data with multiple reputable sources.
- **Ask Key Questions:** Who is the author? What is their authority? When was it published? Why is this source being used?
- **Document Your Findings:** Keep a record of sources used, especially when making decisions based on the information.
- **Use Tools:** Use fact-checking tools, databases and AI responsibly to supplement your information evaluation process.

A **professional approach** to evaluating information includes careful verification, critical thinking and a structured approach to organizing and documenting findings. This protects both personal and organizational credibility.

Never skip evaluation due to:

- time pressure
- routine
- assumptions

# TOPIC 3 – ORGANISING & MANAGING INFORMATION AND DATA

# Why Organisation Is a Professional Competence

In professional environments, **organising information** is not a technical detail but a core work competence that directly affects performance.

**Data organization** is essential for efficiency, productivity, and data security. In the workplace, it ensures that:

- Information is easy to access quickly and confidently when needed.
- Errors are minimized because data is well-structured and easily validated.
- Collaborate effectively with colleagues
- Security risks are reduced as organized data prevents accidental exposure.

# Folder Structure Logic

**Effective Folder Structures:** One of the best ways to organize data is by creating a clear and consistent folder structure. Some key guidelines include:

- **Categorization:** Group files by project, department, or date to make it easy to find what you need.
- **Consistency:** Always follow the same naming and filing system for each project, so files are easier to locate.
- **Subfolders:** Break down large projects into subfolders for specific tasks, making it easier to keep track of different aspects of a project.

A professional folder structure should reflect the logic of work:

- **By project** → when work is project-based
- **By function** → when tasks are repetitive (e.g. finance, HR)
- **By process stage** → when workflows follow phases

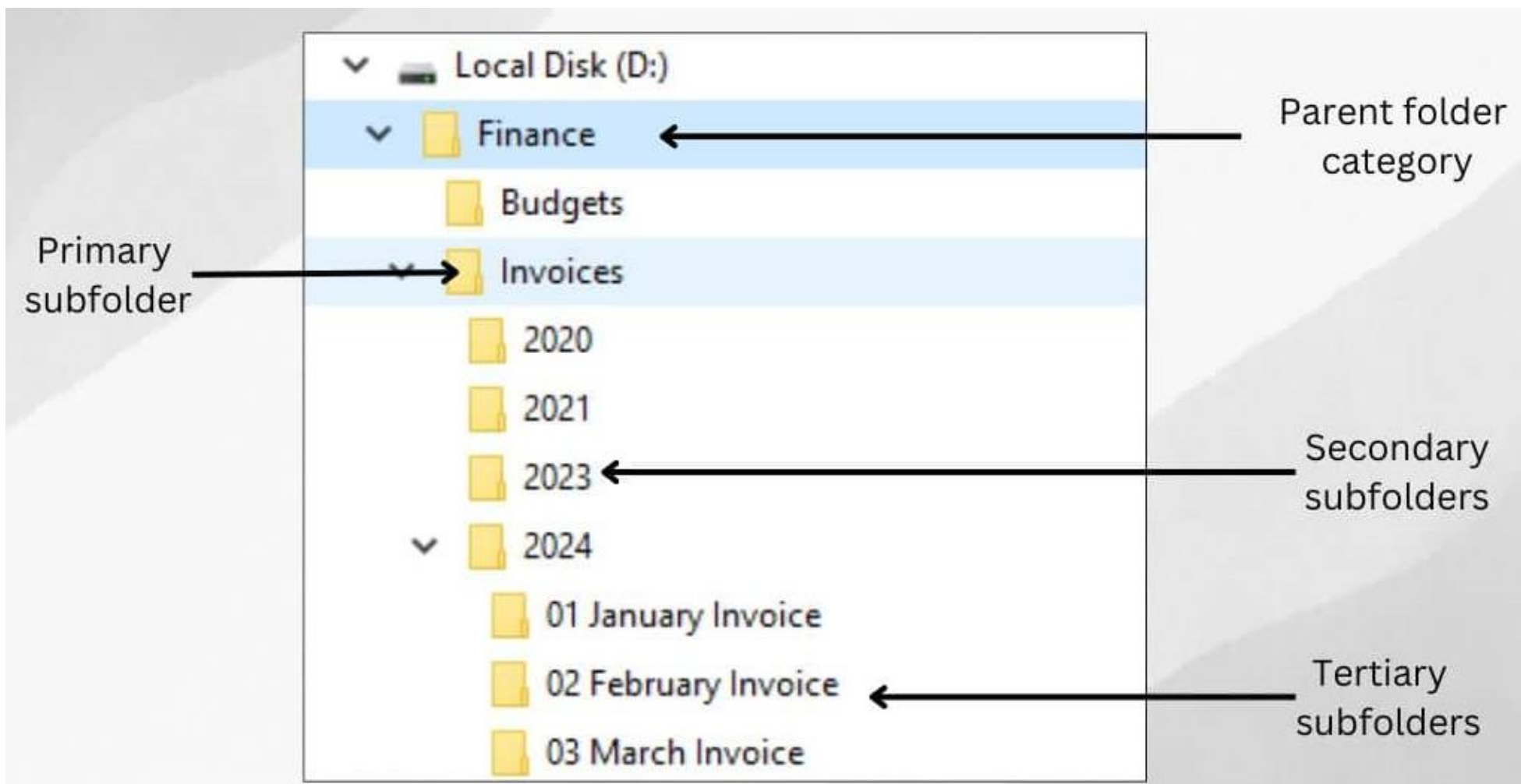
**Example Structure:** *Project → Phase → Document Type → Version*

A well-structured folder system reduces confusion, ensures efficient data retrieval, and helps prevent the loss of important files.

## Best Practices:

- Keep it simple and intuitive.
- Use descriptive names for folders and files to make their contents clear.
- Avoid unnecessary subfolders and complex hierarchies that make the system harder to navigate.
- Ensure your folder structure supports collaboration, with appropriate permissions and access levels.

# An example of grouping folders by category



# Naming Conventions for Files

Consistent naming conventions help ensure that files are easy to identify and retrieve.

Consider these guidelines:

- **Be Descriptive:** Include key details such as project name, date, version number, and content type. Example: *"ClientXYZ\_ProjectReport\_2023-10-15\_V1"*.
- **Keep it Simple:** Avoid overly long names and unnecessary details. The goal is to make the file easily identifiable at a glance.
- **Avoid Special Characters:** Special characters (e.g., !, @, #) can cause issues in some systems. Stick to letters, numbers, and hyphens.
- **Use Consistent Date Formats:** Always use the same date format (e.g., YYYY-MM-DD) so that files are organized chronologically.

Why Naming Conventions Matter:

- **Clarity:** Properly named files are easier to understand and access.
- **Consistency:** Standardized naming prevents confusion when multiple people are managing files.
- **Version Control:** Including version numbers in filenames allows for easy tracking of changes.

# What is Version Management?

**Version management** involves organizing files so that you can track the **evolution** of a document over time. It helps to:

- **Prevent confusion** when multiple versions of the same document exist.
- **Keep a record** of changes made to the file.
- **Track the most recent version** of a document.

## Best Practices for Version Control:

- **Include Version Numbers:** Always label each version of the file (e.g., "v1", "v2", "final") to keep track of updates.
- **Use Cloud Systems with Built-In Version Control:** Cloud storage platforms like Google Drive or OneDrive automatically track version history.
- **Limit Revisions:** Avoid excessive version creation unless necessary. Use clear, deliberate updates to ensure clarity.

Example: A marketing team working on a proposal should label their files as "Proposal\_ClientXYZ\_v1", "Proposal\_ClientXYZ\_v2", etc. This keeps everyone on the same page and prevents confusion about the current version.

By using version control, you ensure that you are always working on the most recent, up-to-date file, minimizing errors and confusion. Example: Report\_v1 → Report\_v2 → Report\_final

# Common Mistakes in Data Organization

## Common Data Organization Mistakes:

- **Overcomplicating Folder Structure:** Creating too many subfolders or unnecessary divisions can make it harder to find files.
- **Inconsistent Naming:** Changing naming conventions or using vague names can make it difficult to know what a file contains.
- **Storing Files in Random Places:** Saving files in random locations instead of a consistent folder structure leads to lost or misplaced files.
- **No Backups:** Failing to back up data can lead to permanent loss in case of system failures.

## How to Avoid Mistakes:

- Keep the folder structure **simple** and **intuitive**.
- Use a **consistent naming system** across all files and documents.
- **Backup regularly** to avoid data loss.

Common mistakes in data organization lead to inefficiencies and frustrations. Following simple best practices can significantly enhance your data management.

# What is Structured Data? (Extended)

**Structured data** refers to data that is organized in a **predefined format** such as rows, columns and tables allowing it to be easily processed and analysed.

## Characteristics of Structured Data:

- **Organized:** Data is organized in rows and columns, making it easy to input, query and analyze.
- **Consistent:** Each entry follows a similar format, such as dates, numbers or text.
- **Easy to Process:** Because the data is predictable, it can easily be processed using automated tools like Excel or Google Sheets.

Example: A **customer database** with columns for name, email, phone number and purchase history is an example of structured data.

Structured data is **ideal for analysis** because its uniformity allows it to be easily queried, sorted and analyzed.

# What is Unstructured Data? (Extended)

**Unstructured data** refers to information that does not follow a predefined format and is difficult to organise and analyse systematically.

Examples: *emails, PDFs, chat messages, notes*

Most information initially exists as **unstructured data**.

**Although there are some problems:**

- difficult to search
- hard to compare
- easily lost

Example: *Customer requests in emails vs structured CRM system.*

Convert important unstructured data into structured formats.

Unstructured data is useful for communication — but risky for decisions.

# From Unstructured to Structured Data

Professional work requires transforming information: **Input → Processing → Use**

Example: Emails / notes → Spreadsheet / system → Decision

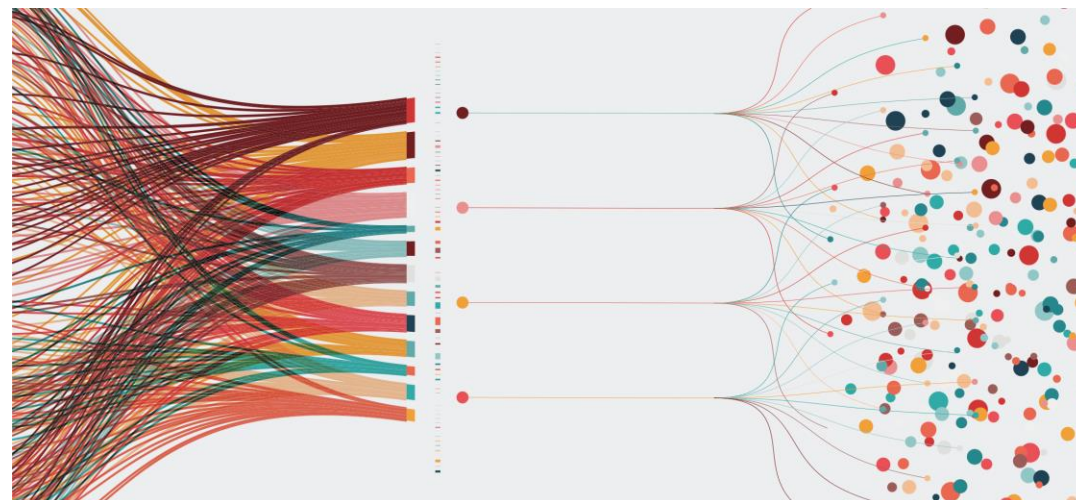
Example Workflow: Customer orders (emails) → entered into spreadsheet → analysed for trends

## Why This Step Matters

- reduces ambiguity
- improves traceability
- supports automation

Skipping structuring leads to:

- inconsistent decisions
- loss of information



The transition from unstructured to structured data is where **professional control begins**.

# Spreadsheets as Structured Data Tools

Spreadsheets (Excel, Google Sheets) are core tools for:

- organising structured data
- analysing patterns and trends
- supporting operational and financial decisions

## Core Functions

- data entry
- sorting and filtering
- formulas and calculations
- data visualisation

## Workplace Applications

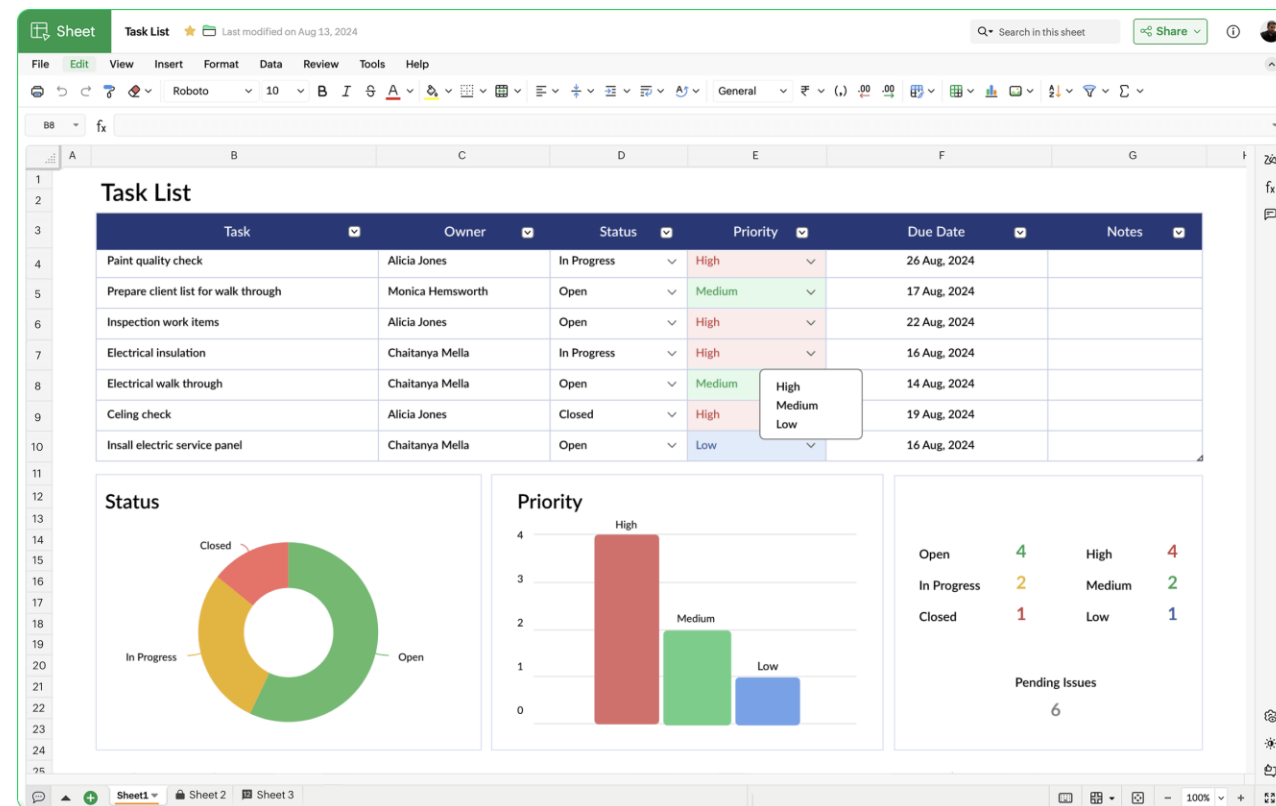
- sales tracking
- inventory management
- budgeting
- reporting

Using spreadsheets without structure leads to:

- inconsistent data
- unreliable outputs

Spreadsheets are not just storage tools — they are **decision-support systems**.

On [Microsoft Excel Training \(Official Guide\)](#) you can find official tutorials on structuring, analysing and managing data effectively.



# Designing a Spreadsheet Correctly

## Key Design Principles

- **One column = one type of data**
- (e.g. Date, Amount, Customer Name – never mixed)
- **Consistent format per column**  
(e.g. all dates in same format, all values numeric)
- **No empty or mixed fields** (avoid gaps, merged cells, or combined data)
- **Use clear headers** (each column must describe exactly what it contains)
- Example:
  - ✗ Incorrect: “12/03 – John – 250€” in one column
  - ✓ Correct: Date | Name | Amount (separate columns)

## Good structure:

- enables sorting and filtering
- supports formulas and automation
- reduces interpretation errors

Most spreadsheet problems do not start in formulas, they start in structure design.

### Risks

Poor design leads to:

- calculation errors
- inconsistent analysis
- inability to reuse data

### Correct Practice

- plan structure before entering data
- keep formats simple and standardised
- review layout before use

# Data Quality and Consistency

High-quality data is essential for reliable analysis and decision-making. Even well-structured data becomes ineffective if quality is not maintained.

## Core Dimensions of Data Quality

- **Accuracy** → values are correct and verified
- **Completeness** → no missing or partial entries
- **Consistency** → same format across all records
- **Reliability** → data can be trusted for decisions

## Common Issues in Practice

- mixed date formats (e.g. DD/MM vs MM/DD)
- inconsistent currencies (€ vs \$ vs text)
- missing values or incomplete rows
- duplicate or conflicting entries

Poor data quality leads to:

- incorrect calculations
- misleading reports
- poor or risky decisions

Data quality is not a technical issue, it is a **decision reliability issue**.

### Correct Practice

- standardise formats before use
- apply validation rules (e.g. numeric-only fields)
- review and clean data regularly
- check for duplicates and inconsistencies

# Human Factor in Data Management

Most data-related problems are not caused by tools, but by **human behaviour and decision-making patterns**.

## Common Behaviours

- rushing data entry
- skipping structure or validation
- relying on memory instead of systems
- inconsistent working habits

## Underlying Causes

- time pressure
- routine (“we always do it this way”)
- cognitive overload
- lack of awareness or training

## Workplace Impact

- repeated errors
- inconsistent datasets
- reduced trust in information
- increased need for corrections

## Correct Practice

- follow clear and consistent procedures
- apply standard rules across all tasks
- verify data before using it
- build habits of checking and reviewing

Technology does not eliminate risk — it shifts responsibility to **human judgement and behaviour**.

# Synthesis: From Data to Reliable Decisions

Effective data management is a structured process that connects information handling with professional decision-making.

## **Integrated Process**

- 1. Structure data correctly**
- 2. Ensure quality and consistency**
- 3. Identify and prevent errors**
- 4. Apply disciplined working practices**
- 5. Enable fast and reliable retrieval**

## **Operational Flow:**

Data → Structure → Quality → Analysis → Decision → Action

# TOPIC 4 – CLOUD STORAGE & DATA MANAGEMENT

# Understanding Cloud Storage in the Workplace

**Cloud storage** refers to saving data in an online environment rather than on physical hardware (e.g., local hard drives). Cloud platforms like **Google Drive**, **OneDrive**, and **Dropbox** allow users to store, access and share files remotely. In simple words cloud storage refers to storing and managing data on **remote servers accessible via the internet**, instead of local devices.

## Benefits of Cloud Storage:

- **Accessibility:** Files are accessible from any device connected to the internet, enabling flexibility for remote work and travel.
- **Collaboration:** Multiple users can access, edit, and collaborate on documents in real time. This is essential for teamwork, especially in SMEs where employees may work across different locations.
- **Scalability:** Cloud storage allows businesses to **scale** their storage needs as the company grows, without needing to invest in additional physical hardware.

Example: A project team working on a **shared document** in **Google Drive** can all make updates in real-time, ensuring everyone has the latest version without having to manually send files back and forth.

# How Cloud Storage Changes the Way We Work

## Traditional Approach (Local Storage)

- files stored on personal computers
- limited access
- manual sharing (email, USB)
- multiple versions of the same file

## Cloud-Based Approach

- shared access in real time
- single version of truth
- continuous updates
- integrated collaboration

## Workplace Example:

- *Before: File\_v1 → File\_v2 → Final\_v3 → FINAL\_FINAL*
- *Now: One shared document → continuously updated*

Cloud transforms work from individual tasks → collaborative processes.

# Core Functions, Collaboration & Control in Cloud Data Management

Cloud systems are not passive storage —they actively shape how work, collaboration and decisions are performed.

## Core Functions (What Cloud Systems Enable)

- **Storage & Organisation:** Structured folders, consistent naming and categorisation
- **Access & Permissions:** Control who can view, edit or share information
- **Version Control:** Track, review and restore changes over time
- **Search & Retrieval:** Fast and reliable access to files when needed

## Collaboration in Practice

- multiple users working on the same file
- real-time updates and shared visibility
- continuous tracking through version history

Cloud efficiency depends on **how well it is managed — not just used.**

In cloud environments: **Collaboration + Control = Reliable Outcomes**

### Correct Practice

- assign clear roles (owner / editor / viewer)
- always check and manage access permissions
- use version history actively
- avoid uncontrolled simultaneous editing
- maintain clear structure and naming conventions

# Risks in Cloud Storage and Data Sharing

Cloud environments introduce specific risks related to **access, sharing and control**.

## Common Risks

- uncontrolled access permissions
- accidental sharing with wrong users
- data exposure through public links
- loss of control over file versions
- data exposure
- external access

Most issues result from:

- misunderstanding permissions
- rushing sharing actions
- lack of verification

In cloud environments **Access = Control = Responsibility**.

### Correct Practice

- always check access settings
- avoid “anyone with link” unless necessary
- review sharing before sending
- regularly audit shared files

# Best Practices for Cloud Data Management

To work effectively with cloud systems, professionals must follow structured practices:

- define roles and responsibilities
- communicate changes clearly
- use shared documents responsibly

## Workflow Discipline

- verify before sharing
- update files consistently
- maintain version clarity

Cloud efficiency depends on **discipline, consistency and responsibility**.

### Key Practices

- organise folders clearly and consistently
- use standard naming conventions
- control access permissions carefully
- avoid duplication of files
- regularly review and clean storage

# TOPIC 5 – ADVANCED CASE-BASED APPLICATION



# Case Scenario 1: Managing Supplier Data for Decision-Making

You are working as a junior operations assistant in a small trading company.

Your Responsibilities are:

- maintaining supplier records
- updating pricing data in spreadsheets
- storing documents in the company cloud system

Your manager asks you to:

- update supplier pricing information
- prepare a comparison report
- upload and share it in the cloud

You are working with:

- multiple spreadsheet versions
- emails with updated prices
- files stored in different folders
- unclear naming conventions

You must complete the task **quickly** because a purchasing decision depends on your report.

In real work situations, data is often **incomplete, scattered and time-sensitive**.

**What is your first priority before starting the task?**

# Analysis of Case Scenario 1: Managing Supplier Data

To handle this situation professionally, you should follow a structured approach:

## Step 1 – Clarify the Objective

- What is required? → Supplier comparison for decision-making
- What is critical? → Accuracy and updated pricing

## Step 2 – Validate Information Sources

- compare spreadsheet data with email updates
- identify outdated or inconsistent information
- prioritise the most recent and reliable sources

## Step 3 – Structure the Data

- create a clean spreadsheet
- define clear columns (supplier, price, date, terms)
- ensure consistency in format

## Step 4 – Ensure Data Quality

- check for missing or incorrect values
- verify calculations
- avoid duplication

## Step 5 – Store and Share Correctly

- save in correct cloud folder
- use proper naming convention
- check permissions before sharing

A professional does not work with the first available data but they validate, structure and verify before acting.

Reliable decisions depend on controlled data, not fast assumptions.

## Case Scenario 2: Managing Customer Data in a Spreadsheet

You are working as a **junior administrative assistant** in a service company.

Your Responsibilities are:

- updating customer records
- maintaining a spreadsheet with transactions
- preparing basic performance summaries

You are asked to:

- update customer transaction data
- calculate monthly totals
- send a summary report to your supervisor

You notice:

- missing values in some rows
- inconsistent date formats
- duplicated entries
- unclear formulas already used in the spreadsheet

The report will be used for **financial planning**, so accuracy is critical.

Any mistake may lead to:

- incorrect financial decisions
- loss of trust

Spreadsheets are often trusted even when they contain **hidden errors**.

**What is the most critical action before using the data?**

# Analysis of Case Scenario 2: Managing Customer Data

This situation requires careful handling of data quality and spreadsheet integrity.

## Step 1 – Identify Data Issues

- locate missing values
- detect duplicates
- check inconsistent formats

## Step 2 – Clean the Data

- standardise formats (dates, currency)
- remove duplicates
- fill or flag missing data

## Step 3 – Review Spreadsheet Structure

- confirm columns are correctly defined
- ensure one data type per column
- avoid mixed or unclear fields

## Step 4 – Validate Calculations

- check formulas and ranges
- test results with sample data

## Step 5 – Prepare Reliable Output

- ensure final report reflects correct data
- review before sharing

Never trust a spreadsheet without checking its **structure, quality and formulas**.

Spreadsheets create an illusion of accuracy but reliability depends on **data quality control**.

## Case Scenario 3: Working with Shared Files in the Cloud

You are working as a **team assistant** in a small project-based company.

### Your Responsibilities are:

- supporting document preparation
- collaborating with team members
- managing files in a shared cloud folder

Your team is preparing a project report.

### You must:

- review the document
- make updates
- share it with the project manager

### You find:

- multiple versions of the same file
- unclear file names (Final\_v2, Final\_NEW, Final\_Updated)
- team members editing different versions

### You are not sure:

- which version is correct
- who made the latest changes
- which file should be sent

The report must be delivered **within the next hour**.

Cloud tools simplify collaboration — but can create confusion without control.

**What is your first step before editing or sharing the file?**

# Analysis of Case Scenario 3: Cloud Collaboration and Version Control

This situation highlights the importance of **control in cloud environments**.

## Step 1 – Identify the Correct Version

- check version history
- identify latest update
- confirm with team if needed

## Step 2 – Establish Control

- identify file owner
- ensure only authorised edits

## Step 3 – Avoid Duplication

- stop working on multiple files
- consolidate into one shared version

## Step 4 – Apply Clear Naming

- rename file consistently
- remove confusing duplicates

## Step 5 – Verify Before Sharing

- confirm correct version
- check permissions
- ensure final accuracy

In cloud systems, clarity and control are more important than speed. Collaboration requires **structure, ownership and discipline**.

## Case Scenario 4: Searching and Evaluating Information for a Task

You are working as a **junior employee** in a **small company**.

### Your Responsibilities are:

- searching for external information
- supporting operational decisions
- collecting and summarising data

### You are asked to:

- find information about a new supplier
- check compliance requirements
- provide a recommendation

### You find:

- different information on websites
- a blog article with useful details
- an AI-generated summary
- an official source with complex content

### Difficulty

- information is inconsistent
- some sources are easier to understand
- others are more reliable but complex

Your manager expects a **quick and clear answer**.

Choosing the wrong source may lead to:

- incorrect decisions
- compliance issues

The easiest information is not always the **most reliable**.

**Which source would you trust first and why?**

# Analysis of Case Scenario 4: Evaluating Information Sources

This situation requires **critical evaluation and professional judgement**.

## Step 1 – Identify Source Types

- official source → high reliability
- blog / AI → lower reliability
- mixed sources → require validation

## Step 2 – Evaluate Information

- check accuracy
- verify author and origin
- confirm update date

## Step 3 – Compare Sources

- identify differences
- prioritise authoritative information
- cross-check key facts

## Step 4 – Avoid Common Mistakes

- do not choose easiest source
- do not rely on one source
- do not trust unverified AI output

## Step 5 – Form a Justified Recommendation

- base decision on verified information
- explain reasoning

A professional does not select information based on convenience but based on **reliability and relevance**.

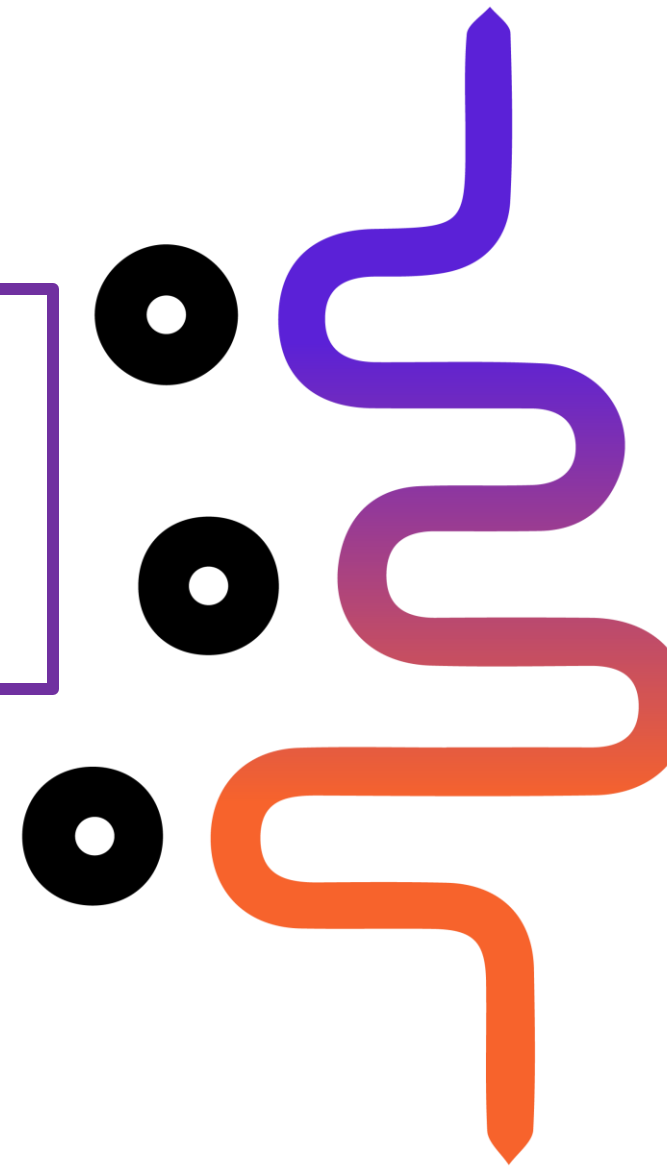
Critical thinking is the ability to **question, compare and justify decisions**.

# Sources

- European Commission (2022) *Digital Economy and Society Index (DESI) 2022: Human Capital*. Available at:  
<https://digital-strategy.ec.europa.eu/en/policies/desi> (Accessed: 31 March 2026)
- University of North Carolina (UNC) (2023) *Evaluating Information Sources*. Available at:  
<https://guides.lib.unc.edu/evaluating-info/evaluate> (Accessed: 31 March 2026)
- IBM (2023) *Data Management: Risks of Poor Information Handling*. Available at:  
<https://www.ibm.com/topics/data-management> (Accessed: 31 March 2026)
- Microsoft (2024) *Excel Training: Structuring and Managing Data Effectively*. Available at:  
<https://support.microsoft.com/en-us/excel> (Accessed: 31 March 2026)

# Digital Tools & AI for Everyday Professional Tasks

## Unit 3



# Identifying Digital Needs: Start with the Task

Effective tool use begins with task analysis, not tool selection.

## Key Factors to Consider:

- **Frequency:** How often is this task performed?
- **Collaboration:** Does it involve multiple people?
- **Complexity:** Does it require heavy data or simple text?
- **Output:** What does the final deliverable look like?

Using a "power tool" (like complex CRM) for a "hand-tool" task (a simple contact list) increases effort and reduces efficiency.

**Right Tool + Right Task = Efficiency**

**Wrong Tool + Wrong Task = Overhead & Wasted Time**

# Categories of Digital Work

Workplace tasks fall into four functional categories:

## 1. Production: Content Creation & Synthesis

- *The engine room where ideas are turned into tangible assets.*
- **Word Processing:** Drafting long-form documents, reports, and proposals (e.g., **Microsoft Word, Google Docs**).
- **Visual Storytelling:** Creating high-impact decks and presentations for stakeholders (e.g., **PowerPoint, Canva**).
- **Creative Design:** Professional-grade media, prototyping, and brand assets (e.g., **Adobe Creative Cloud, Figma**).

## 2. Communication: Information Flow & Connectivity

- *The "connective tissue" that ensures the right person has the right info at the right time.*
- **Synchronous (Real-time):** Instant messaging for rapid troubleshooting and "office chatter" (e.g., **Slack, Microsoft Teams**).
- **Asynchronous (Delayed):** Formal correspondence and record-keeping that doesn't require an immediate reply (e.g., **Outlook, Gmail**).
- **Virtual Presence:** Bridging the gap for remote teams through face-to-face interaction (e.g., **Zoom, Google Meet**).

# Categories of Digital Work

## 3. Organization: Planning & Resource Management

- *The framework that manages the two most scarce resources: Time and Focus.*
- **Time Management:** Managing individual and team availability (e.g., **Google Calendar**, **Calendly**).
- **Project & Task Management:** Tracking progress, assigning accountability, and hitting deadlines (e.g., **Asana**, **Trello**, **Monday.com**).
- **Knowledge Management:** Centralizing "tribal knowledge" and internal documentation (e.g., **Notion**, **Obsidian**, **Confluence**).

## 4. Analysis & Data: Insights & Decision Making

- *The analytical layer that converts raw numbers into strategic action.*
- **Spreadsheet Modeling:** Quantifying logic, budgeting, and organizing structured data (e.g., **Excel**, **Google Sheets**).
- **Business Intelligence (BI):** Visualizing complex data sets through interactive dashboards (e.g., **Tableau**, **Power BI**).

**Each category requires different tools and logic.**

# Selecting Productivity Tools Strategically

Tool selection must be based on business logic, not popularity. Evaluate every tool against these four critical pillars:

- **Cost-Efficiency vs. Purchase Price:** Do not just look at the subscription fee. Calculate the **Return on Investment (ROI)**. Does the manual time saved by the team justify the monthly cost?
- **Interoperability & Integration:** Does the tool "talk" to your existing ecosystem? A tool is only productive if it syncs seamlessly with your primary systems (e.g., Google Workspace, Microsoft 365, or existing CRM/ERP).
- **Learning Curve & Usability:** How intuitive is the interface? Estimate the "Total Time to Proficiency." A complex tool that requires weeks of training may cause a temporary drop in team productivity.
- **Security & GDPR Compliance:** Is the data handled according to EU standards? Verify that the tool offers encrypted storage, multi-factor authentication (MFA), and clear data-handling policies.

# The "Free" Tool Trap in Professional Environments

Free tools often appear cost-effective but create hidden risks.

## Key Issues with Free Tools:

### 1. Lack of Essential Security Features

- Free tools often lack the necessary **security features** required to protect business data.
- Example: *A free cloud storage platform may not offer **data encryption**, leaving sensitive business information vulnerable to breaches.*

### 2. No Technical Support

- Free tools typically offer **limited or no technical support**, meaning that any problems you face may go unresolved for longer periods.
- Example: *If an issue arises with a free tool, you might face extended downtime without a dedicated support team, leading to **lost productivity**.*

# The "Free" Tool Trap in Professional Environments

## 3. Creating "Data Silos" and Lack of Integration

- Many free tools **do not integrate** with other business systems or software. This creates **data silos**, making it difficult to share information across platforms, leading to inefficiencies and miscommunication within teams. **Data silos** refer to situations where data is stored in isolated systems that do not communicate or integrate with each other.
- Example: *Using a free contact management tool that doesn't sync with your email or CRM system results in **disjointed data**, causing errors and delays.*

## 4. Increased Hidden Costs in Time and Security Risks

- Although free tools may seem cost-effective initially, the hidden costs such as **security gaps** and lack of support can lead to **greater expenses** in the long run. Time spent troubleshooting, resolving integration problems, and managing security risks can cost more than a paid tool.
- Example: *If your free tool becomes inadequate as your business grows, you may need to switch to a paid version or another tool, resulting in **hidden switching costs**.*

# Linking Tool Use with Efficiency

**The Logic: Efficiency = (Value of Output) / (Time + Effort)**

The goal is to ensure that the tools you use help you achieve high-quality results with minimal time and effort. Tools should improve output without adding unnecessary complexity.

Operational errors are costly and often arise from manual processes, such as:

- Manual data entry errors
- Lost emails
- Version conflicts in collaborative work

Example: *By automatically updating contact info in your CRM, you avoid manually updating records, reducing errors and saving time. This integration ensures that data is consistent across systems and up-to-date.*



| Category                             | Professional Tools                              |
|--------------------------------------|-------------------------------------------------|
| AI Reasoning & Advanced Drafting     | ChatGPT, Gemini, Claude.ai, MS Word             |
| Information Research & Synthesis     | Perplexity, Google Scholar, Claude (PDF)        |
| Data Literacy & Analysis             | MS Excel, Google Sheets, Power BI               |
| Visual Design & Storytelling         | MS PowerPoint, Canva, Adobe Express, Midjourney |
| Workflow & Knowledge Management      | Trello, Asana, Notion, MS Planner               |
| Collaboration & Meeting Intelligence | MS Teams, Slack, Otter.ai, Fireflies.ai         |



# Workplace Optimization Logic

Optimization begins with identifying workflow bottlenecks.

**Bottlenecks** are the obstacles in your workflow that slow down the overall process. These can arise from inefficient tools, manual tasks, or poor collaboration.

- **The 80/20 Rule**

- "20% of your tools likely produce 80% of your value."
- Identify and focus on the tools that truly enhance your work and consider reducing or eliminating those that add little value.

- **Automation vs. Manual Work**

- **Automation:** Streamlining tasks using digital tools to eliminate repetitive manual work.
- **Manual Work:** Tasks that require human intervention, often leading to slower processes and more chances for error.

# The Role of AI in Modern Workflows as a Productivity Partner

AI is no longer optional — it is a core productivity layer.

To leverage Artificial Intelligence effectively, professionals must shift their mental model: Generative AI (ChatGPT, Claude and Gemini) is not a search engine; it is a **Reasoning Engine**.

- **Core Capabilities (The "What"):**

- **Synthesis:** Summarizing complex reports or lengthy email threads.
- **Production:** Drafting initial versions of emails, proposals, or social media content.
- **Ideation:** Brainstorming creative solutions and project outlines.
- **Technical Support:** Generating and debugging code or reformatting data structures.

- **Critical Constraints (The "What Not"):**

- **Factuality:** It does not guarantee truth; it predicts patterns (risk of "hallucinations").
- **Context:** It lacks "common sense" and cannot understand specific SME internal context unless explicitly provided.
- **Authority:** It cannot take professional responsibility for its outputs.

Treat Generative AI as a highly capable but slightly unreliable intern. It can perform 80% of the heavy lifting in seconds, but it requires a human supervisor to verify, refine, and authorize the final 20%.

# AI for Summarising

AI reduces cognitive load in routine tasks:

- Summarising long documents
- Writing emails and reports
- Structuring content

Example: *You are presented with a 50-page industry report, but you only have 10 minutes before a critical strategy meeting.*

- **AI Action:** Upload the document or provide the text to an LLM with a Context-Specific Prompt: "Extract the top 5 key findings and 3 actionable risks for a small-scale manufacturing firm from this report. "
- **Benefits:** Instant reduction of information overload.
- Use AI to save time on low-value tasks — focus on decisions.

How much time could you save weekly by using AI for summarization?

# AI for Organising Work

AI tools can support the organisation of work by structuring information, tasks and processes into clearer and more manageable formats.

AI can be used to structure:

- **Task lists** → breaking down complex activities into smaller, actionable steps
- **Workflows** → organising processes into logical sequences (e.g. step-by-step procedures)
- **Data formats** → transforming unstructured information into tables, summaries or categories
- AI supports:
  - **Clarity** → improves understanding of tasks and responsibilities
  - **Prioritisation** → helps identify what is urgent or important
  - **Planning** → supports better time management and workflow coordination

An employee uses AI to:

- convert meeting notes into a structured task list
- assign priorities and deadlines

This improves efficiency and reduces the risk of missed actions.

# AI for Drafting & Ideation

AI is particularly useful for:

- **Overcoming “blank page” situations** → starting complex or high-stakes tasks
- **Generating multiple variations** → exploring tone, structure and approach
- **Supporting idea development** → structuring concepts and communication strategies

Example: *Prompt: “Generate 5 variations of a polite but firm email requesting a 10% discount from a long-term supplier.”*

The user can compare different tones (formal, collaborative, assertive) and select the most appropriate.

## Benefits

- **Rapid Prototyping** → explore multiple options in seconds
- **Linguistic Precision** → access professional phrasing and vocabulary
- **Cognitive Offloading** → reduce effort on drafting and focus on decisions

# The AI-Human Collaboration Model (workflow diagram)

You are the "Pilot"; AI is the "Co-pilot."  
The pilot is always responsible for the landing.

**1. Human:** Sets the goal, provides context, defines constraints.

**2. AI:** Generates drafts, offers variations, processes large data.

**3. Human:** Evaluates, fact-checks, refines, and takes responsibility.

# Prompt Engineering: The Art of Instruction

A prompt is not just a question, it is a **command**. In the age of AI, the quality of your output is strictly limited by the precision of your input.

| Element        | The "Vague" Approach (Weak)                         | The "Architect" Approach (Strong)                                                                                                                                                                                    |
|----------------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Prompt     | "Write a business plan."                            | "Act as a <b>Senior Startup Consultant</b> . Outline a <b>3-phase market entry strategy</b> for a <b>SaaS company</b> launching in the <b>EU</b> . Focus on <b>GDPR compliance</b> and <b>localized marketing</b> ." |
| The Result     | Generic, "fluffy" text that requires heavy editing. | High-level, actionable strategy tailored to your specific constraints.                                                                                                                                               |
| The Difference | Lacks context, role, and specific goals.            | <b>Persona + Context + Specific Goal + Constraints.</b>                                                                                                                                                              |

# The CREATE Framework for Prompts

- Character: Who should the AI be? (e.g., "Senior Accountant")
- Rrequest: What is the task? (e.g., "Analyze this budget")
- Examples: Provide a template or style.
- Audience: Who is it for? (e.g., "The Board of Directors")
- Type: What format? (e.g., "Table," "Email")
- Extras: Constraints (e.g., "Under 200 words," "No jargon")

Using a framework like CREATE ensures you don't forget the context that makes AI useful.

Practice this framework until it becomes second nature.

# Example of a Well-Crafted Prompt Using CREATE

- **Character:** "Assistant Manager"
- **Request:** "Summarize this month's sales performance."
- **Examples:** "Provide the summary in bullet points with key metrics like total sales, top-performing products, and areas for improvement."
- **Audience:** "Sales team"
- **Type:** "Bullet points"
- **Extras:** "Keep the summary under 150 words. Use clear and simple language."

## Explanation:

- **Character:** We define the role of the AI (Assistant Manager) to give it the proper context.
- **Request:** The task is clear: summarize the sales performance for the month.
- **Examples:** We specify how we want the output (bullet points with key metrics).
- **Audience:** We define the target audience (Sales team) to ensure the AI adapts the tone and content.
- **Type:** We want the summary in bullet points, which is easy to read and digest.
- **Extras:** The word limit and language style constraints ensure the output is concise and clear.

# Evaluating AI Output the four-point verification

To ensure professional-grade deliverables, AI outputs must never be used raw.

Apply a rigorous four-point verification checklist before any output is finalized:

- **Empirical Accuracy & Data Integrity:** Are specific figures, dates, and proper names correct?
- **Stylistic Alignment & Tone:** Does the text sound "robotic" or overly generic?
- **Contextual Relevance & Utility:** Does the output actually solve the specific workplace problem, or is it a generic response?
- **Ethical & Safety Compliance:** Does the content adhere to the company's ethical guidelines and GDPR standards?

# Navigating the AI Maturity Curve: Fluency vs. Mastery

- **AI Fluency (The "How"):** Developing the linguistic and technical ability to communicate with the AI model (Proficiency in Prompt Engineering and the CREATE framework).
- **AI Mastery (The "Should" & "Why"):**
  - Knowing when AI is the right tool and when a human-only approach is superior.
  - The ability to systematically verify outputs and detect "**Hallucinations**"—statistically plausible but factually incorrect information.

AI frequently generates errors regarding specific financial figures, legal citations, proper names and events occurring after its last training update.

**"AI-Wisdom":** Most users stop at fluency, accepting AI output at face value. A professional at the Mastery level recognizes that LLMs are probability engines, not database queries. Being "AI-Wise" means maintaining a healthy skepticism and a robust verification protocol.

# AI Ethics: Transparency and Ownership

## Key principles:

- **Transparency:** Be honest if a deliverable was 100% AI-generated.
- **Bias:** AI can repeat societal biases (gender, race). A professional must correct these.
- **Ownership:** You own the output only if you have significantly edited and verified it.

Your professional "signature" means you stand behind the content, regardless of how it was drafted.

➤ *Should a student be allowed to use AI for an essay? Should an employee use it for a report including real data? Is there a difference?*

Ethics is about building trust. If you hide your AI use, you damage your professional identity.

# Self-Diagnosis: Identifying Your Digital Gaps

Small and Medium Enterprises (SMEs) face unique digital challenges:

- Limited IT support (You are often your own support).
- Need for high versatility (Multitasking across different toolsets).
- Direct impact on revenue (Inefficiency costs the company immediately).



You cannot improve what you cannot measure. Before we begin, we must measure the "Gap."

- Do you use only the tools you know, or the tools that are best?
- Can I automate a recurring report?
- Can I distinguish between an AI "hallucination" and a fact?

Real professional growth starts with admitting which technical areas we have been avoiding. Most professionals use only 10% of their software's capabilities.

# The Digital Improvement Plan (DIP) – (Part 1: Tools & AI)

## Phase 1: Identification

- List 3 digital tasks that are currently bottlenecks, tasks that take too much of your time or cause significant frustration.

## Phase 2: Tool Research

- Identify one specific tool (whether it is an AI agent or standard software) that has the potential to solve or automate each of those tasks.

## Phase 3: Learning Goals

- Set a concrete "micro-learning" target for this week.
- Example: Watch 3 tutorials on Excel Macros to automate weekly reporting.

A Digital Improvement Plan is a living document of your professional evolution. It shouldn't be static; it grows as your skills do.

## Case Scenario: The “Fast but Wrong” Workflow

Maria works in a small SME as an administrative assistant. She needs to prepare a **client update email and a short report** based on internal data.

To save time, she:

- Uses **AI to draft the email and report**
- Copies **client data directly into the AI tool**
- Uses a **free file-sharing tool** to send the report
- Does **not review the AI output carefully**

The task is completed in **15 minutes instead of 1 hour**.

### What Happens Next:

- The email contains **inaccurate information (AI hallucination)**
- Sensitive client data was **exposed through the AI tool**
- The file is shared with the **wrong version**
- The client notices inconsistencies and questions reliability

**What went wrong in this workflow? Identify at least 3 critical mistakes.**

# Scenario Analysis: What Should Have Been Done?

## 1. Task Analysis Failure

- No evaluation of: sensitivity of data and the required accuracy.
- Wrong assumption: “AI = safe shortcut”

## 2. Misuse of AI

- Entered **sensitive data into public AI tool**

## 3. Poor Tool Selection

- Used **free, non-integrated tool**
- Result: version confusion and lack of control

## 4. Lack of Output Validation

- No final check before sending leads to reputational risk

### Correct Professional Workflow:

- ✓ Remove/anonymize sensitive data before AI use
- ✓ Use **approved tools only**
- ✓ Verify AI output (accuracy + tone)
- ✓ Confirm final version before sharing

Professional work is not about speed. It is about **controlled, reliable outcomes**.

# External Resources & Further Learning

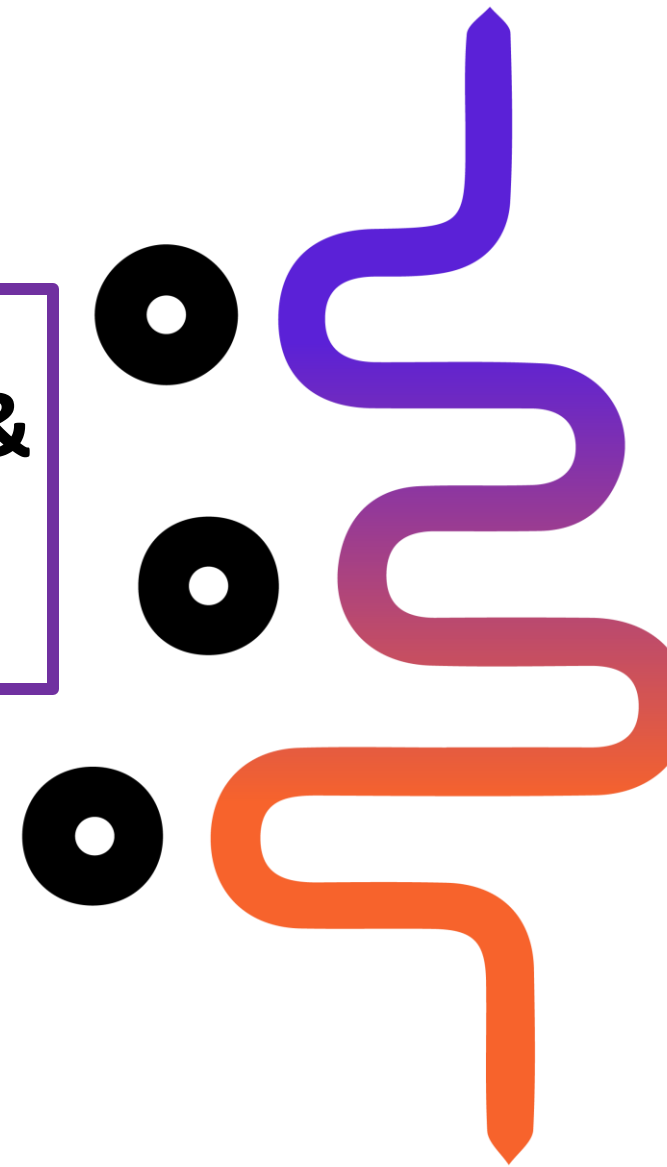
To deepen your skills in digital tools and AI, explore the following **trusted resources**:

- [OECD AI Principles](#)
- [5 AI for Work Tips and Tricks – YouTube](#)

This video demonstrates how AI tools can support everyday professional tasks such as drafting, summarising, and organising work. It highlights practical ways to integrate AI into daily workflows while maintaining control and quality.

# Digital Communication, Collaboration & Professional Identity

## Unit 4



# The Cost of Poor Digital Communication

Poor digital communication creates operational inefficiencies and affects both workflow and professional relationships.

## Impact of Poor Communication

- **Misinterpretation** → unclear messages lead to wrong understanding
- **Delays** → tasks need clarification or rework
- **Errors** → incorrect execution of instructions
- **Loss of trust** → reduced confidence in communication quality

### Example:

*Unclear email → task misunderstood → incorrect output → time lost*

One unclear message can affect multiple people.

Unclear communication creates hidden operational costs.

# Principles of Professional Digital Communication

## Key Principles

- **Clear** → no ambiguity
- **Concise** → no unnecessary information
- **Structured** → easy to follow
- **Purpose-driven** → focused on outcome

### Correct Practice

- define your message before writing
- focus on what the reader needs

## Example:

Well-structured message → faster decision → fewer errors

If the reader has to guess, communication has failed.

# Email Communication – Professional Standards

## Structure of a Professional Email

- Clear subject line
  - Purpose in first sentence
  - Structured message (short paragraphs)
  - Clear action or expectation
- Example: *Subject: Update Required – Project X. Please review and confirm changes by Friday.*

### Risk

- unclear emails → delays and confusion
- long messages → reduced attention

## Recommended Tools

- Outlook / Gmail (for email domains)
- Grammarly (AI tool for tone & clarity)

# Drafting a Professional Email

## Core Structure

- **Salutation** → professional and context-aware (*Dear [Name], Hello [Name]*)
- **The Purpose (“Why”)** → state the reason for the email in the first 1–2 sentences
- **The Request (“Ask”)** → clearly define what is needed and use bullet points for multiple requests
- **The Sign-off** → professional closing + signature (*Name, Role, Organisation, Contact details / LinkedIn*)

## Example:

*“Hello Maria,  
I am contacting you to request the updated project file for review.  
Could you please send:*

- *the final version*
- *the latest budget file”*

# Digital Body Language: Tone in Written Communication

In digital communication, tone is conveyed through wording, punctuation and visual cues, not voice or facial expression.

## Key Elements

- **Emojis**
  - acceptable in informal internal communication (Teams, Slack)
  - avoid in formal or external emails
- **Punctuation** → excessive use (!!!, ???) appears unprofessional
- **Wording Choices** → short or abrupt messages may be misinterpreted

## Example:

- “Fine.” → may feel abrupt or negative
- “That works for me.” → clearer and more neutral

# Netiquette in Professional Environments

Netiquette defines appropriate behaviour in digital communication.

## Key Rules

- use professional tone
- avoid informal language in formal contexts
- respect response time

Tone is often misunderstood in digital communication

### Risk

- tone misinterpretation
- perceived unprofessional behavior

### Correct Practice

- review tone before sending
- adapt communication to context

# Communication Channels – Choosing the Right One

Different communication tools serve different purposes.

## Channel Selection

- **Email** → formal communication
- **Chat (Teams, Slack)** → quick coordination
- **Meetings** → complex discussion

The tool shapes the message.

### Risk

wrong channel → wrong outcome

### Correct Practice

choose the channel based on purpose and urgency

# Collaboration in Digital Workspaces

Modern work depends on shared and connected digital tools.

## **Key Elements**

- shared documents
- real-time collaboration
- cloud-based systems

## **Benefits**

- speed
- transparency
- coordination

## **Recommended Tools**

- Google Workspace
- Microsoft Teams / SharePoint
- Notion

# Risks in Digital Collaboration

## Common Risks

- version conflicts
- unclear ownership
- overwriting content
- data exposure
- Example: *Multiple users editing → lost changes*

## Correct Practice

- assign ownership
- track changes
- use controlled access

Collaboration without control creates chaos

# Controlling Who Can Do What

## Access Levels

- **Viewer** → read only
- **Commenter** → feedback
- **Editor** → full access

## Risk

- too much access → data exposure
- too little access → inefficiency

## Correct Practice

- assign permissions carefully

# Safe Practices in Data Sharing

Secure file sharing ensures that organisational data is accessed, used and distributed in a controlled and protected way.

Sharing files incorrectly can lead to:

- unauthorised access
- data leaks
- loss of control over information

## Best Practices

- use **organisation-approved platforms** → ensures security, logging and compliance
- avoid **unsecured channels** → e.g. personal email, messaging apps
- control **sharing settings** → restrict access, disable download where needed

## Recommended Tools

- **OneDrive / SharePoint** → enterprise-level control
- **Google Drive** → flexible sharing & collaboration

# Maintaining Accuracy in Shared Work

Version control ensures that all users work on the correct and most up-to-date version of a document.

## **Without Version Control**

- confusion about latest version
- duplicated files
- overwritten or lost work

## **Correct Practice**

- use **shared documents instead of attachments**
- enable **track changes / version history**
- avoid downloading and re-uploading files

## **Tools**

- Google Docs (real-time editing)
- Microsoft 365 (version history & collaboration)

# How You Are Perceived in Digital Environments

Your digital identity is the professional image you project through your behaviour, communication and online presence.

## Key Elements

- **Communication style** → clarity, tone, professionalism
- **Online presence** → profiles, posts, shared content
- **Behaviour in tools** → collaboration habits, responsiveness

## Example (Workplace Context)

- Consistent, clear communication → trusted professional
- Unclear or informal behaviour → reduced credibility

# Managing Your Digital Footprint

Every digital action leaves a trace that can influence your professional reputation.

## What It Includes

- emails and attachments
- internal messages (Teams, Slack)
- social media activity

### Example:

*Unprofessional comment in internal chat → shared externally → reputational impact*

# Boundaries in Digital Communication

Healthy boundaries in digital communication support productivity, well-being and safer decision-making.

## Risks of “Always-On” Culture

- burnout and fatigue
- reduced concentration
- increased errors

### Example:

- *Constant notifications → distraction → careless mistakes*

## Correct Practice

- define availability and response times
- manage notifications
- avoid non-urgent communication outside working hours

# Professional Responsibility in Communication

Ethical communication ensures that information is shared responsibly, respectfully and in a way that protects individuals, organisations and data.

## Core Principles

- **Respect** → communicate professionally, avoiding offensive, informal or inappropriate language
- **Transparency** → provide clear, honest and complete information and avoid misleading or incomplete messages
- **Confidentiality** → protect sensitive, personal or organisational data and share information only with authorised individuals
- **Example** Sharing internal company information in a public channel or forwarding an email without checking permissions

## Risk

- breach of confidentiality
- reputational damage
- loss of trust within teams or clients
- potential legal implications

## Correct Practice

- communicate clearly and honestly
- verify recipients before sharing information
- respect data sensitivity and privacy rules

# Shared Accountability in Digital Work Environments

Collaboration requires each participant to take responsibility for their actions, contributions and communication.

## Key Responsibilities

Each user is responsible for:

- **Accuracy** → ensuring information shared is correct and reliable
- **Data Handling** → using, storing and sharing data responsibly
- **Communication Clarity** → providing clear instructions and updates

Example: A team member uploads incorrect data into a shared file without verification. This affects the entire team's work.

## Risk

- propagation of errors across the team
- confusion and rework
- reduced trust in shared outputs

## Correct Practice

- verify information before sharing
- communicate changes clearly
- take ownership of contributions
- support team coordination

In collaborative work, individual actions affect collective outcomes

# Understanding Why Communication Breaks Down

Communication failures often result from human behaviour, poor structure or inappropriate tool selection.

## Common Causes

- **Assumptions** → expecting others to understand without explanation
- **Lack of Clarity** → vague or incomplete messages
- **Poor Structure** → unorganised information
- **Wrong Tools** → using inappropriate communication channels

Example: *Sending a complex task via chat instead of a structured email leads to confusion and missed details.*

## Risk

- misunderstandings
- delays in execution
- incorrect outcomes
- reduced efficiency

## Correct Practice

- communicate clearly and explicitly
- structure information logically
- choose the appropriate communication channel
- Most communication failures are preventable

# Best Practices for Collaboration

## Core Guidelines

- ✓ **Define roles** → assign responsibility for tasks and content
- ✓ **Use shared tools** → ensure all team members work in the same environment
- ✓ **Communicate changes** → inform others about updates or edits
- ✓ **Track versions** → maintain control over document evolution

## Risks of Poor Practice

- confusion and duplicated work
- inconsistent information
- loss of control over content

Collaboration is effective only when it is structured and controlled

# Virtual Meeting Etiquette: Professional Behaviour in Online Meetings

Virtual meetings require the same level of professionalism as face-to-face interactions.

## Key Practices

- **Preparation** → check microphone, camera and connection before the meeting
- **Environment**
  - use a clean or blurred background
  - ensure appropriate lighting and positioning
- **Engagement**
  - avoid interrupting
  - use features such as “Raise Hand”
- **Mute Discipline** → stay muted when not speaking to avoid distractions

Example:

*Unmuted microphone → background noise → disrupted meeting*

# Case Scenario – Miscommunication

## Scenario

- A team collaborates on a shared document:
- no clear owner
- multiple users editing simultaneously
- no communication about changes

## What Happens

- overlapping edits
- conflicting versions
- loss of information

## Result

- confusion among team members
- errors in content
- delays in project completion

Lack of structure leads to operational inefficiency

# Scenario Analysis – What Went Wrong?

## Core Issues

- **No ownership** → no accountability for content
- **No structure** → lack of organised workflow
- **Poor communication** → no updates or coordination

## Impact

- duplicated effort
- inconsistent outputs
- reduced productivity

## Correct Practice

- ✓ assign clear roles and responsibilities
- ✓ use version control tools
- ✓ communicate updates and changes
- ✓ define workflow before collaboration

Effective collaboration requires structure, not just participation

# Final Check Before Sharing or Collaborating

A final review ensures that communication and collaboration are clear, accurate and appropriate.

## Checklist

Before sending or sharing:

- ✓ **Is it clear?** → is the message understandable?
- ✓ **Is it complete?** → does it include all necessary information?
- ✓ **Is it appropriate?** → is tone and format suitable?
- ✓ **Is access correct?** → do the right people have the right permissions?

## Example:

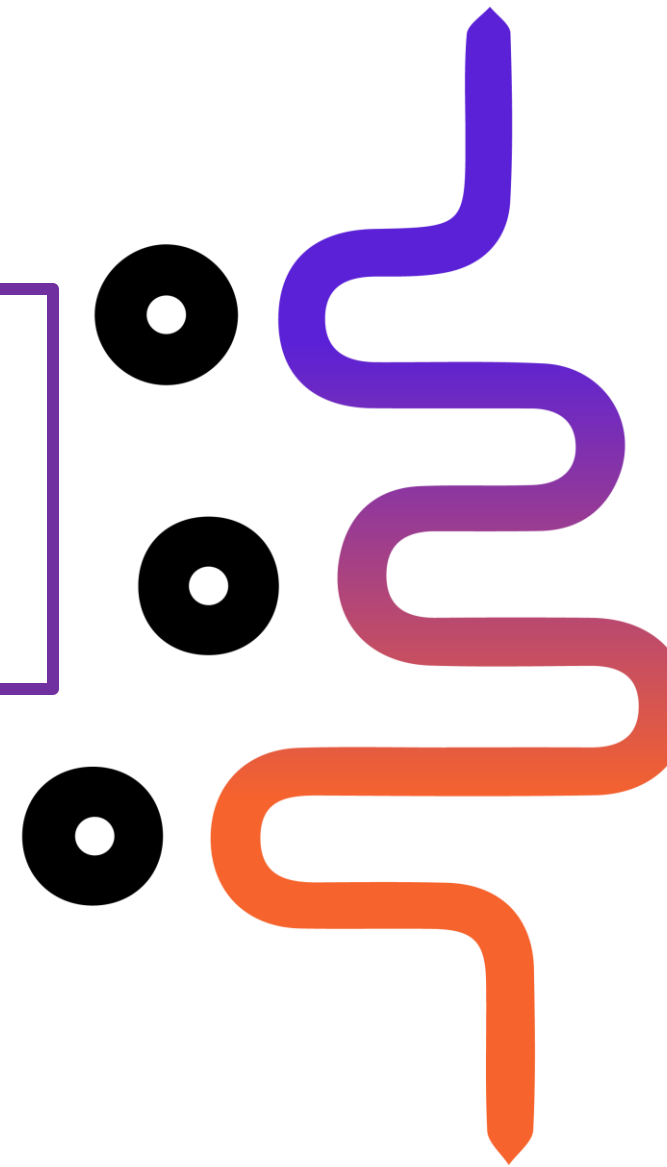
Before sharing a file:

- check clarity
- verify content
- confirm access permissions

Prevents errors and miscommunication.

# **Creating & Editing Digital Content for Workplace Deliverables**

## Unit 5



# What Defines Professional Digital Content?

Professional content is defined by:

- **Clarity** → easy to understand, without ambiguity or unnecessary complexity
- **Structure** → logically organized, with clear flow and sequencing
- **Accuracy** → correct and verified based on reliable information
- **Purpose** → aligned with task goals, audience and objective

Poor content leads to:

- Miscommunication
- Wrong decisions
- Loss of credibility
- Confusion in workflows

If your content is unclear, your work is unclear. Professional communication reflects professional competence and directly influences trust and performance.

# Structuring Content for Impact

Professional content should follow a simple and consistent flow:

- **Purpose** → What is this document or message trying to achieve?
- **Key Message** → What is the most important point the reader must understand?
- **Supporting Information** → What data, explanation or evidence supports the message?
- **Conclusion / Action** → What should happen next? What is expected from the reader?

Example:

- **Poor structure** → *long, unorganised text without headings or clear focus*
- **Effective structure** → *clear sections, logical flow, highlighted key points*

The second enables faster understanding and better decisions.

# Text vs Visual Balance

Effective content uses:

- **Text** → to explain ideas, provide detail and ensure accuracy
- **Visuals** → to highlight key points, simplify complexity and guide attention

The goal is **complementarity**, not competition.

Example:

- *A report with only dense text → difficult to read and interpret*
- *A report with structured text + simple visuals (icons, diagrams) → easier to understand and act upon*

## Risk of Imbalance

- **Too much text** → cognitive overload, reduced attention, missed information
- **Too many visuals** → distraction, loss of focus, unclear message

### Correct Practice

- use visuals to **clarify key ideas**, not decorate content
- keep text concise and structured
- highlight essential information visually
- ensure visuals directly support the message

# Designing Readable Documents

## Key Readability Principles

To improve readability:

- **Short paragraphs** → make content easier to scan and understand
- **Clear headings** → guide the reader through the structure
- **Bullet points** → highlight key information and improve clarity
- **Consistent formatting** → creates a professional and predictable reading experience

## Example:

- *A document with long text blocks and no structure → difficult to follow*
- *A document with headings, spacing and bullet points → easy to read and act upon*

# Creating Professional Presentations

## Key Principles

Effective presentations:

- **Focus on key messages** → highlight what is essential, not everything that is known
- **Avoid information overload** → limit content to what can be easily understood
- **Use visual hierarchy** → guide attention through titles, spacing and emphasis

## Recommended Tools

- **Microsoft PowerPoint** → standard professional presentation tool
- **Canva** → user-friendly templates and visual design support
- **Google Slides** → collaborative and cloud-based presentation creation

### Risk of Poor Presentation Design

- audience confusion or disengagement
- key messages lost or misunderstood
- reduced credibility and impact

### Correct Practice

- simplify content to essential points
- structure slides clearly and consistently
- support text with meaningful visuals
- design presentations to guide understanding, not just display information

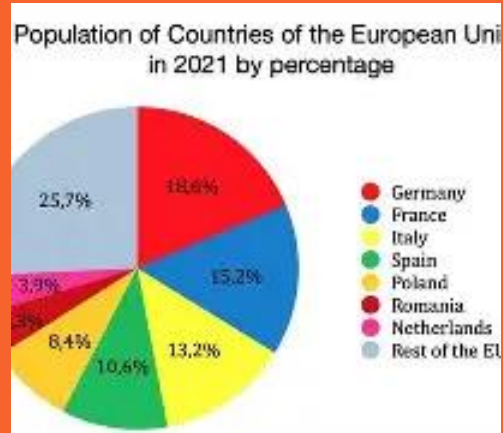
# Document Engineering

Effective document engineering includes:

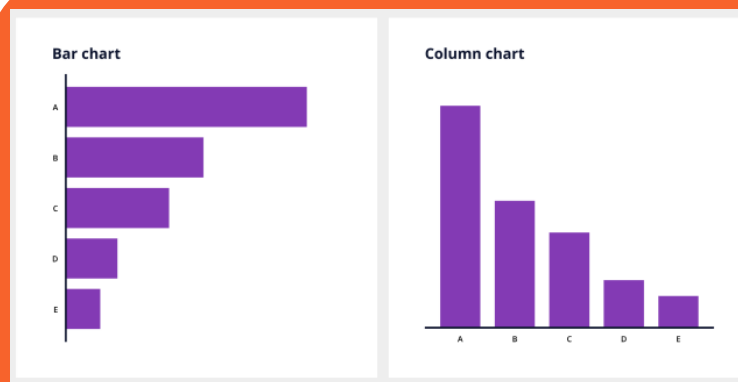
- **Templates** → predefined formats that ensure consistency across documents
- **Standard structures** → clear organisation (e.g. introduction, main content, conclusion)
- **Consistent formatting** → uniform fonts, spacing, headings and layout
- Example:
  - ***Random document*** → *inconsistent layout, unclear structure, difficult to follow*
  - ***Company template-based report*** → *structured sections, consistent design, easy to navigate*

Structured documents improve usability and professionalism.

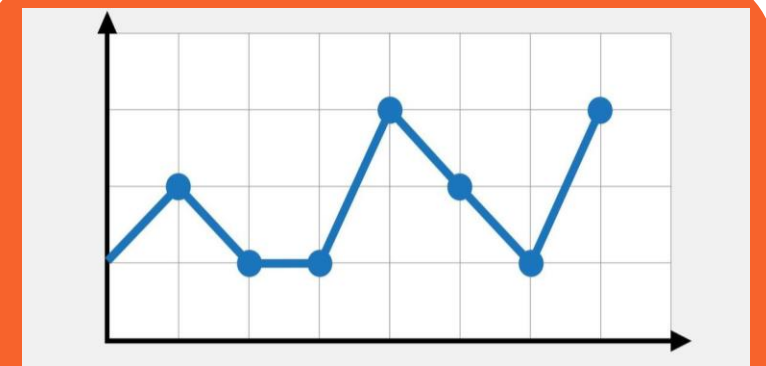
# Data Visualization: Turning Numbers into Insights



**Pie Charts:** Best for showing parts of a whole (keep to <5 categories).



**Bar/Column Charts:** Best for comparisons between different groups or time periods.



**Line Graphs:** Best for showing trends over time.



# Editing for Quality

Effective editing includes:

- **Grammar** → correct language use to ensure professionalism and credibility
- **Clarity** → clear and understandable wording without ambiguity
- **Accuracy** → correct facts, data and information
- **Tone** → appropriate style for the audience and context
- Example:
  - *A draft email sent without review → unclear message and potential misunderstanding*
  - *A reviewed and edited message → clear, precise and professional communication*

Editing improves both understanding and impact.

Writing is drafting — editing is professionalism.

# Using AI Responsibly in Professional Content Development

AI can assist with:

- **Drafting** → generating first versions of content
- **Rewriting** → improving clarity, tone or structure
- **Structuring** → organising ideas into logical formats

## Ethical Use Principles

- **Do not copy blindly** → always review and adapt content
- **Verify accuracy** → cross-check with reliable sources
- **Avoid bias** → critically evaluate AI-generated content

# Respecting Ownership in Professional Digital Content

Copyright provides automatic legal protection to original works (text, images, code, music) from the moment of creation. In the EU, all original content is **protected by default**.

- Professional use of content requires:
  - **Respect for ownership** → recognising that content belongs to its creator
  - **Avoidance of plagiarism** → not copying or presenting others' work as your own
  - **Use of licensed material** → ensuring permission for professional use

**The Myth of "Public" Images:** Just because an image is on Google does **not** mean it is free to use professionally.

Example: *An employee uses an image found online in a company presentation without checking licensing rights.*

This may result in legal and reputational consequences.

## Risk

- legal action or financial penalties
- violation of intellectual property rights
- reputational damage for the organisation
- loss of professional credibility

## Correct Practice

- use licensed or royalty-free content
- always check usage rights before using material
- credit sources where required
- assume content is protected unless clearly stated otherwise

# Navigating Creative Commons (CC) Licenses

- **CC-BY (Attribution)** → content can be used, but the creator must be credited
- **CC-NC (Non-Commercial)** → cannot be used for business, marketing or profit-related activities
- **CC-ND (No Derivatives)** → content can be used, but cannot be modified or edited
- **CC0 (Public Domain)** → no rights reserved; free to use without restrictions

Example: *An SME uses an image with a **CC-NC license** in a marketing campaign. This violates the license because the use is commercial.*

# Navigating Creative Commons (CC) Licenses



BY (attribute)



Share Alike



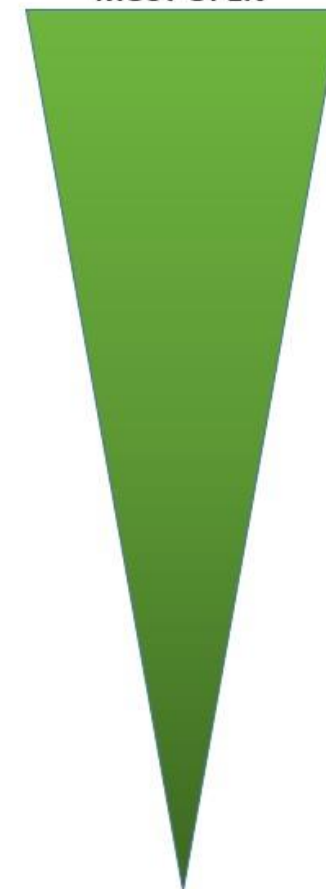
Non-Commercial



No Derivatives



MOST OPEN



LEAST OPEN

# Ethical Sourcing: Professional Asset Libraries

## High-Quality Sourcing Options:

- **Images:** Unsplash, Pexels, Pixabay (ensure you check the license per image).
- **Icons:** The Noun Project, Flaticon, Icons8 (often require attribution).
- **Fonts:** Google Fonts (Open Source and safe for business).
- **Internal Libraries:** Building a shared folder of pre-approved, licensed assets for your team to prevent accidents.
- Example: A team prepares a presentation using:
  - licensed images from Unsplash
  - icons from Flaticon (with attribution)
  - company-approved templates

This ensures both legal compliance and professional visual consistency.

# Avoiding Plagiarism

**Plagiarism** refers to copying text or ideas without credit.

- **Professional Paraphrasing** → expressing ideas in your own words while citing the source (e.g. “According to ENISA (2024)...”)
- **Quoting** → using exact words with quotation marks and attribution (used selectively for emphasis)
- **Self-Plagiarism** → reusing your own work in different contexts without disclosure

Example: *An employee copies content from an online report into a company document without referencing the source.*

This is plagiarism and may damage credibility and trust.

# Ethics Check – Paraphrasing vs AI Generation

Professional content creation requires transparency regarding how content is produced, especially when using AI tools.

## The Professional Standard

- **Original Research** → human-driven content based on analysis and cited sources
- **Paraphrased Content** → human interpretation of existing knowledge with proper attribution
- **AI-Generated Content** → machine-assisted output that must be reviewed, adapted and disclosed when significant **The Transparency Rule**

If a client expects **expert judgement**, delivering fully AI-generated content without disclosure:

- misrepresents the work
- may breach professional trust or contract terms

# Workflow for Content Creation

## Step-by-Step Workflow

1. **Define Purpose** → What is the goal of the content? Who is the audience?
2. **Draft Content** → Create the initial version focusing on key ideas
3. **Structure Content** → Organise information logically (headings, sections, flow)
4. **Edit and Refine** → improve clarity, tone, grammar and consistency
5. **Validate** → verify accuracy, check sources and ensure suitability for use

# Quality Control & Self-Diagnosis

Quality control is the final step in content creation, ensuring that output meets professional, organisational and communication standards.

Before sharing, confirm that your content is:

- ✓ **Clear** → easy to understand, without ambiguity
- ✓ **Accurate** → correct, verified and up to date
- ✓ **Structured** → logically organised with clear flow
- ✓ **Audience-appropriate** → tone and level match the target audience

## Self-Diagnosis (Professional Check)

- Do I use **templates and structured formats** or random formatting?
- Can I present information **clearly and logically**?
- Do I verify **sources, data and permissions** before use?
- Is my content **accessible and understandable** to others?
- Do I follow a **final review routine before sharing**?

# Case Scenario: Poor vs Professional Content

Nikos works in a small company and is asked to prepare a **client presentation** for a new service.

He creates the presentation by:

- Copying text directly from different sources
- Using **AI to generate slides without editing**
- Adding too much text on each slide
- Using inconsistent fonts, colors and layout
- Including images without checking copyright

The presentation is delivered on time.

## What Happens Next:

- The client finds the presentation **confusing and difficult to follow**
- Some information appears **inaccurate or irrelevant**
- The visual design looks **unprofessional**
- The company's credibility is reduced

# Scenario Analysis: What Should Have Been Done?

## 1. Lack of Structure

- No clear message or flow
- Too much information per slide
- ✓ Correct Practice: One idea per slide + logical sequence

## 2. Misuse of AI

- AI content used without validation
- No adaptation to context
- ✓ Correct Practice: AI = draft → Human = refinement + validation

## 3. Poor Visual Design

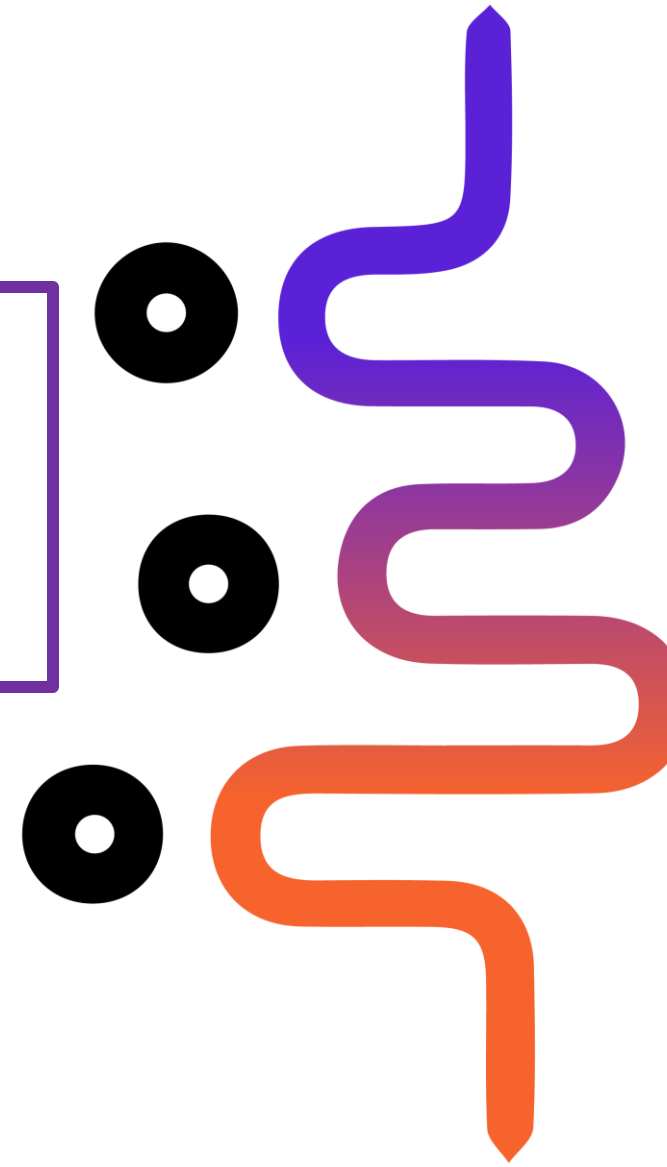
- Inconsistent formatting
- Overloaded slides
- ✓ Correct Practice: Use templates + visual hierarchy

## 4. Ethical Issues

- Unverified content
- Possible copyright violations
- ✓ Correct Practice: → Use licensed content + check accuracy

# Solving Basic Technical Problems

## Unit 6



# The Cost of Technical Problems

Technical problems directly affect productivity, workflow and organisational performance.

## **Their negative impact:**

- Lost productivity
- Missed deadlines
- Frustration and stress
- Reputational impact

## Example:

*File not syncing → wrong version sent to client and this impacts both accuracy and trust*

Small technical issues can create large business consequences

# Types of Common Technical Problems

Most workplace technical problems fall into a limited number of categories that can be identified and addressed systematically.

## Common Categories

- **Connectivity Issues** → problems with internet, Wi-Fi or VPN access
- **Access Problems** → login errors, permission restrictions, account issues
- **Software Errors** → application crashes, bugs or performance issues
- **Data Issues** → missing files, sync problems, version conflicts

### Example:

*A user cannot access a shared document → problem may relate to permissions, sync or connectivity*

If you can classify the problem, you can solve it faster.

# The Troubleshooting Mindset

Effective troubleshooting requires logical thinking and structured problem-solving.

## Key Principles

- calm thinking
- step-by-step logic
- avoiding assumptions

## Wrong Approach

- random clicking
- trial-and-error guessing

## Correct Approach

- structured diagnosis
- controlled testing

Example: *Clicking multiple settings randomly → problem worsens*

Guessing increases problems — logic solves them.

# The Core Troubleshooting Logic

## Step-by-Step Process

1. Identify the problem clearly
2. Check basic causes (connection, access, system)
3. Test solutions step-by-step
4. Confirm resolution

### Example:

*Cannot open file → check access → test alternative → confirm fix*

Always start simple before moving to complex solutions

# The RRU Rule (Restart–Reconnect–Update)

Many technical issues can be resolved through basic system actions.

## Key Actions

- **Restart** → clears temporary memory issues
- **Reconnect** → restores network access
- **Update** → fixes bugs and compatibility issues

## Example:

*Application not responding → restart → issue resolved*

Simple solutions solve most problems

# Diagnosing Before Acting - Ask Before You Fix

## Key Questions

- What changed?
- When did the problem start?
- Is it only me or system-wide?

## Example:

*If only one user is affected → likely local issue*

*Multiple users affected → system problem*

# Hardware vs Software vs Network

## Distinction

- **Hardware** (The Physical) → These are the tangible components you can touch—cables, devices, monitors, and peripherals like mice or keyboards
- **Software** (The Digital) → These are the applications, operating systems, and programs that run on your hardware
- **Network** (The Invisible) → This is the bridge that connects your devices to the internal company system or the wider internet

## Example:

*Mouse not working → check cable or battery first*

The secret to professional troubleshooting is isolation. By testing one layer at a time, you can pinpoint the exact cause of the failure.

# Solving Connectivity Issues

## Checks to Perform

- Internet connection → Start at the source. Is the entire building offline, or is it just your device? Check if other websites load or if your colleagues are experiencing the same issue
- Wi-Fi status → Ensure your Wi-Fi is actually toggled on. Sometimes, a simple "Off and On" toggle is enough to force the device to re-scan for the strongest signal
- Router status → If you are working from home or in a small office, look at the hardware. Are the lights green? A red or blinking light usually indicates a service provider issue or a need for a physical reboot
- VPN settings → For many professionals, the VPN is the final gate. If your internet works but your company tools don't, your VPN might have "timed out" or failed to authenticate. Disconnect and log back into the VPN to refresh the secure tunnel

## Example:

You try to open a cloud-based report and get a "No Internet" error. Instead of calling IT immediately, you check the router, see it's flashing, and reconnect the network by power-cycling the device. Within two minutes, you are back online without any external help.

# Remote Connectivity Challenges

## Issues

- **weak home Wi-Fi:** Distance from the router, physical barriers, or high network traffic from other household devices can cause "lag" during critical video calls or slow file uploads
- **VPN instability:** Corporate VPNs are essential for security, but they can be temperamental. Frequent disconnections often point to a conflict between your local ISP and the encrypted tunnel
- **Public network risks:** Using Wi-Fi at a café or airport might be convenient, but these networks are often unencrypted, making them a "gold mine" for data theft and cyber-attacks

## Correct Practice

- **Use secure networks:** Always prioritize your password-protected home network. Ensure your router is running the latest firmware and is positioned in a central location.
- **Avoid public Wi-Fi for sensitive tasks:** Never access company databases, financial records, or private client data over a public connection. If you must work in public, always use your VPN.
- **Use mobile hotspot as backup:** If your home internet fails, a mobile hotspot is your professional "Plan B." It is far more secure than a public network and ensures you stay online for important deadlines.

Connectivity = professional reliability

# Resolving Access Problems - Permissions and Authentication

Access problems occur when users cannot reach systems, files or platforms due to authentication or permission issues.

Access issues typically relate to:

- incorrect permissions → this is the most frequent culprit. You may have the link to a file, but your user profile hasn't been granted the specific "view" or "edit" rights required
- expired login → for security reasons, most professional systems require you to re-authenticate periodically. If you've left a tab open for three days, your "session" has likely timed out, even if you look logged in.
- wrong account → many of us juggle multiple digital identities—a personal Gmail, a corporate account, and perhaps a client-specific login. If you try to open a company document while signed into your personal browser profile, the system will block you.

Example:

*User cannot open shared file → file exists but access rights not granted*

Most access problems are permission-related, not technical failures

# Managing Cloud & Sync Issues

Cloud systems depend on continuous synchronisation between local devices and online storage.

## **Common Problems**

- files not updating
- version conflicts (duplicate versions)
- missing data

## **Correct Practice**

- check sync status
- use shared versions
- avoid duplicate files

“Saved” does not always mean “synced”

# Cloud Sync Deep Understanding - Recognising Sync Status Indicators

Cloud systems use visual indicators to show file status.

## Indicators

- blue icon → syncing in progress
- green check → fully synced
- red error → sync problem

Example: Closing laptop before sync completes → file not updated

## Risk

- data loss
- outdated versions
- missing files

## Correct Practice

- confirm sync completion before closing work
- monitor sync errors

# Understanding Software Errors

Software errors occur due to system limitations or outdated environments.

## Common Causes

- outdated software
- system overload
- compatibility issues

Example: *Application crashes → version not compatible with system*

Software problems are often predictable

## Risk

- interruption of work
- data loss
- reduced productivity

## Correct Practice

- update software regularly
- close unnecessary applications
- restart systems when needed

Software problems are often predictable and preventable

# Peripheral Troubleshooting - Devices & Hardware Issues

Many technical issues originate from physical devices.

## Checks

- cables connected properly
- device powered on
- drivers installed/updated

## Example:

*You send a document to the printer, but nothing happens. Instead of digging into your document settings, you restart the device and reconnect the cables. Often, this "physical reset" clears a communication jam, and the printer resumes immediately. Printer not working → restart device → reconnect*

Many issues are physical, not digital.

# Preventive Maintenance - Avoiding Problems Before They Start

## Actions

- **update systems regularly** → software updates are not just about new features; they contain critical security patches and performance fixes. Delaying an update is essentially leaving a door unlocked in your digital office.
- **organize files** → A cluttered desktop and chaotic folder structure don't just slow you down—they slow your computer down. Indexing thousands of loose files puts unnecessary strain on your operating system's resources.
- **clean storage** → A cluttered desktop and chaotic folder structure don't just slow you down—they slow your computer down. Indexing thousands of loose files puts unnecessary strain on your operating system's resources.

Example: Consider two employees. One has a desktop covered in 500 random icons; the other uses a structured folder system. Organized files lead to faster access, which results in fewer errors and less mental fatigue. Organised files → faster access → fewer errors

Prevention is more efficient than repair

# Digital Hygiene

Digital hygiene refers to maintaining systems for optimal performance.

## Practices

- **Remove Unnecessary Files:** Regularly audit your "Downloads" and "Desktop" folders. Delete temporary files, old installers, and documents you no longer need. If you haven't opened a file in a year, it's a candidate for archiving or the trash.
- **Manage Storage Space:** Your operating system needs free space to "breathe" and swap temporary data. If your drive is nearly full, your computer will struggle to perform even basic tasks. Aim to keep at least 15% of your storage free.
- **Disable Unused Startup Apps:** Many programs set themselves to open automatically the moment you turn on your computer. This consumes valuable memory (RAM) before you've even started working.

## Example:

*Too many startup apps → slow system*

Clean systems perform better

# Backup & Data Protection

Backups ensure data recovery in case of failure.

## Practices

- **Save Regularly:** Do not rely solely on "Autosave." Make it a habit to manually save your work during natural breaks in your thought process. This ensures that even a sudden power loss only costs you a few minutes of work, not hours.
- **Use Cloud Backup:** Platforms like OneDrive, Google Drive, or Dropbox provide a continuous safety net. By working within these folders, your files are automatically mirrored on secure remote servers, protecting them from local hardware failure.
- **Maintain Local Copies:** For mission-critical projects, follow the "3-2-1 rule": keep three copies of your data, on two different media types, with one copy off-site (the cloud). Having a local copy on an external drive ensures you can still work even if you lose internet access.

## Example

*Imagine your computer suffers a major system crash an hour before a big deadline. Because you maintained a consistent backup, you simply log into another device and restore your work. What could have been a disaster becomes a minor 10-minute delay.*

We must treat data protection with the gravity it deserves: Data loss equals business loss. Whether it's lost billable hours, missed deadlines, or damaged client trust, the cost of losing data is always higher than the effort of backing it up.

In modern content creation, backup is not optional—it is essential.

# Backup Strategy (3-2-1 Rule)

**To achieve total data security, your strategy must include:**

- **3 Copies of your data:** This includes the primary version you are currently working on and at least two additional backups.
- **2 Different storage types:** Don't keep all your backups on the same device. Use two different media—for example, your computer's internal hard drive and an external drive. This protects you if one piece of hardware fails.
- **1 Off-site copy:** At least one backup must be in a different physical location. In the modern world, this is usually the Cloud. This ensures that even if there is a fire, theft, or flood at your office, your data remains safe and reachable.

## Example

You keep your working file on your Local PC, a secondary copy on an External SSD, and a third copy syncing to the Cloud (like OneDrive or Dropbox).

- Failure is inevitable — preparation prevents disaster

# Human Factor in Technical Problems

Human behaviour is often the root cause of technical problems.

## Causes

Most "user errors" can be traced back to three psychological states:

- **Rushing:** Trying to meet a deadline often leads to skipping essential steps, like checking a sync status or verifying a file destination.
- **Distraction:** Multitasking or working in a cluttered environment increases the likelihood of clicking the wrong button or deleting the wrong folder.
- **Misunderstanding:** Using a tool without reading the basic instructions or understanding its logic leads to predictable failures.

## Example

- Clicking wrong file → data overwritten
- Humans often create technical problems
- Technology fails — but human behaviour often triggers it

# Communicating Technical Issues

Clear communication reduces troubleshooting time.

## What to Include

- **Problem Description:** Be specific. Instead of "I can't log in," say "I am receiving 'Error 404' when trying to access the Client Portal." Detail exactly what you see on the screen.
- **Actions Already Taken:** List what you have already tried. Mention if you have applied the RRU Rule (Restart, Reconnect, Update). This prevents the support team from suggesting steps you've already completed, saving everyone time.
- **Screenshots or Evidence:** A picture is worth a thousand words in troubleshooting. Capture the error message or the visual glitch. This provides the "proof" the technical team needs to diagnose the root cause.

## Example

- “Cannot access file – checked connection and permissions”

Clear reporting = faster solutions

# Escalation Protocols

Escalation is part of professional problem-solving.

## When to Escalate

- cannot resolve issue
- affects multiple users
- involves sensitive data

## Rule

**30-minute rule:** If you cannot solve a technical problem within 30 minutes of focused effort, stop. Continuing beyond this point leads to diminishing returns and wasted billable hours.

Knowing when to stop is a professional skill

# Communicating with IT - Writing a Clear Incident Report

## **Include**

- system/environment
- action attempted
- error message
- steps taken

## **Example**

“Windows 11 – cannot upload file – error 404 – tried restart”

Clear reporting = faster solutions. It transforms a frustrating technical block into a streamlined administrative task.

# Case Scenario – System Failure

## Scenario

- User cannot access shared files before deadline

## The Chain Reaction

- **Panic:** The user experiences "digital panic," losing the ability to think clearly or diagnose the problem.
- **Random Actions:** Without a plan, they start changing random settings, clicking through menus, and disconnecting cables.
- **Deleting Files:** In a misguided attempt to "clear space" or "reset" the folder, they begin deleting files, hoping it will fix the connection.

The consequences of these actions go far beyond a simple access issue:

- **Data Loss:** The random deletions result in permanent loss of work.
- **Significant Delays:** The time spent on random actions was time that could have been used for proper troubleshooting or escalation.
- **Team Disruption:** Colleagues now have to stop their own work to help recover what was lost, affecting the entire department's performance.

Poor decisions under pressure increase damage

# Scenario Analysis

## Steps

- ✓ check connection
- ✓ verify access
- ✓ check sync
- ✓ avoid destructive actions

## Correct Practice

- act logically
- avoid irreversible actions
- Calm logic prevents escalation

# Troubleshooting Checklist

## The Final 5-Step Check

- ✓ restart
- ✓ check connection
- ✓ verify access
- ✓ check updates
- ✓ test simple fixes

Digital resilience is a core professional skill

# Key points

## 1. Digital Safety

1. Protects data, systems, and trust.
2. Main risks: Phishing, Malware, Social Engineering, Weak Authentication.

## 2. GDPR & Data Handling

1. Adherence to GDPR is crucial for personal data protection and legal compliance.
2. Safe handling and storage practices are required.

## 3. Authentication & Device Protection

1. Multi-factor authentication (MFA) and device security are critical to prevent unauthorized access.
2. Regular updates and encryption are essential for device protection.

## 4. File Management

1. Organize files with clear structures to prevent loss or unauthorized access.
2. Use controlled file sharing and data protection measures.

## 5. AI Responsibility

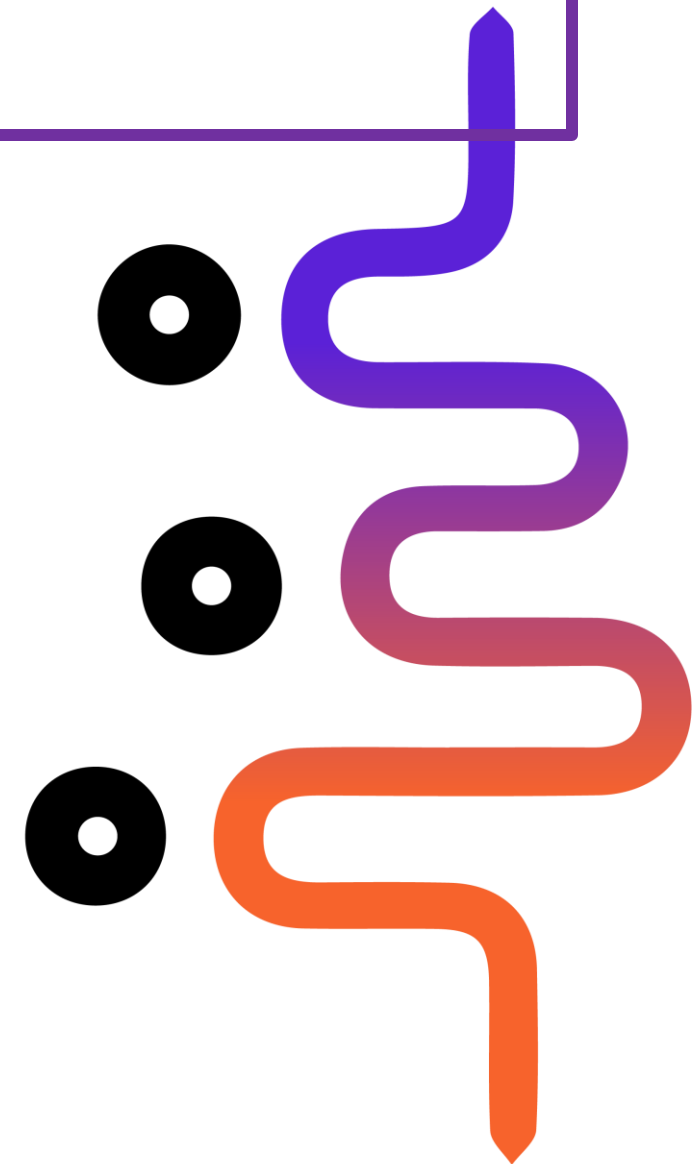
1. Use AI tools responsibly, ensuring GDPR compliance and data protection.
2. Validate AI outputs to avoid errors and misleading results.

## 6. Remote Working & Well-being

1. Use secure networks and devices for remote work.
2. Prioritize digital well-being to prevent overload and stress.

## 7. Technical Problem Solving

1. Follow the "Restart – Reconnect – Update" logic for troubleshooting.
2. Clear communication with IT teams is key for quick issue resolution.





**Co-funded by  
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.