

Unit I: Introduction to Digital Fluency

1. Meaning of Digital Fluency

Digital fluency refers to the ability to use digital technologies confidently, effectively, safely, and responsibly. It involves more than basic computer knowledge; it also includes finding information, communicating online, solving problems using digital tools, and creating digital content.

For example, using a computer to prepare a report, searching for information on Google, attending online classes, and communicating through email are examples of digital fluency.

2. Importance of Digital Fluency

Digital fluency is important because technology is widely used in education, business, banking, communication, and government services. It helps individuals access information quickly, improve productivity, develop professional skills, and participate in the digital economy.

It also enables students to attend online classes, entrepreneurs to promote their products online, and citizens to use digital payment systems and government portals.

Major benefits:

- Improves communication and collaboration.
- Provides easy access to information and learning resources.
- Saves time and reduces paperwork.
- Supports employment, entrepreneurship, and business growth.
- Encourages safe and responsible use of technology.

3. Skills Required for Digital Fluency

Digital fluency requires a combination of technical, communication, information-management, and safety skills.

The major skills include:

- Basic computer skills: Operating computers and using applications.
- Information literacy: Searching, evaluating, and verifying online information.
- Digital communication: Using email, video conferencing, and social media appropriately.
- Content creation: Preparing documents, presentations, spreadsheets, and digital media.
- Problem-solving: Identifying and solving basic technical problems.
- Cybersecurity awareness: Protecting passwords, personal information, and devices.
- Digital citizenship: Behaving ethically and respectfully online.

A digitally fluent person can select appropriate digital tools, use them effectively, and adapt to new technologies.

Unit II: Computer Basics

1. Introduction to Computer Hardware and Software

A computer is an electronic device that accepts data, processes it according to instructions, stores it, and produces useful information. Hardware and software are the two basic components of a computer system.

Hardware refers to the physical parts of a computer that can be touched, such as the keyboard, monitor, mouse, CPU, and printer.

Software refers to the programs and instructions that tell a computer what to do. Examples include Windows, MS Word, Excel, and web browsers.

Hardware and software depend on each other. Hardware cannot perform useful tasks without software, while software requires hardware to operate.

2. Basic Computer Components and Their Functions

Input devices

Input devices are used to enter data and instructions into a computer. Examples include a keyboard, mouse, scanner, microphone, and webcam.

Central Processing Unit (CPU)

The CPU is known as the brain of the computer. It processes instructions and controls computer operations. Its main components include the Arithmetic Logic Unit (ALU), Control Unit (CU), and registers.

Output devices

Output devices present processed information to users. Examples include monitors, printers, speakers, and projectors.

Memory and storage devices

Memory holds data needed for processing. RAM temporarily stores data while programs are running, whereas SSDs, hard disks, and pen drives store data for future use.

3. Introduction to Operating Systems

An operating system (OS) is system software that manages computer hardware and software resources and provides an interface between the user and the computer.

Examples include Microsoft Windows, macOS, Linux, Android, and iOS.

Main functions of an operating system:

- Process management: Manages running programs.
- Memory management: Allocates memory to applications.
- File management: Organises, stores, and retrieves files.
- Device management: Controls devices such as printers and keyboards.
- User interface: Allows users to interact with the computer.
- Security: Supports user accounts, permissions, and access control.

Without an operating system, using a modern computer or smartphone would be much more difficult.

4. Basic File Management

File management refers to organising, storing, locating, copying, moving, renaming, and deleting digital files and folders.

A file is a collection of digital information, while a folder is used to organise files and other folders.

Common file operations include:

- Create: Make a new file or folder.
- Save: Store changes to a file.
- Copy: Create another copy of a file.
- Move: Transfer a file to another location.
- Rename: Change the name of a file.
- Delete: Remove a file.
- Restore: Recover a file from the Recycle Bin or Trash, when available.

Common file extensions include .docx for Word documents, .xlsx for Excel files, .pdf for PDF documents, .jpg for images, and .mp3 for audio files.

Proper file management makes information easier to find and reduces the risk of losing important data. Regular backups are also essential.

5. Introduction to the Internet

The Internet is a worldwide network of interconnected computers and devices that communicate using standard protocols. It allows people to exchange information, communicate, study, shop, and access digital services.

Major uses of the Internet:

- Education through online classes and digital libraries.
- Communication through email, messaging, and video calls.
- Banking, online payments, and shopping.
- Entertainment through videos, games, and music.
- Business promotion, online sales, and customer service.
- Access to government services and public information.

The Internet has made communication faster and information more accessible across geographical boundaries.

6. Introduction to the World Wide Web (WWW)

The World Wide Web is a system of interlinked web pages and digital resources that can be accessed through the Internet using a web browser.

A website is a collection of related web pages, while a web page is an individual page containing information.

Important terms:

- Web browser: Software used to access websites, such as Google Chrome, Safari, and Firefox.
- URL: The address of a web resource.
- HTTP/HTTPS: Protocols used to transfer web content; HTTPS provides an encrypted connection.
- Hyperlink: A clickable link connecting one web resource to another.

- Search engine: A service used to find information on the Web.

The Internet is the underlying global network, whereas the Web is one of the services that operates over it.

Unit III: Introduction to the Internet, Email and Social Media

1. Navigating the Web

Web navigation means moving between websites and web pages to find and use information. A browser provides tools that make this process convenient.

Important browser features:

- Address bar: Used to enter website addresses and search queries.
- Back and forward buttons: Move between previously visited pages.
- Refresh button: Reloads the current page.
- Tabs: Allow several web pages to be opened in one window.
- Bookmarks: Save useful websites for future access.
- Downloads: Store files obtained from websites.

Users should check website addresses carefully, avoid suspicious links, and prefer HTTPS connections when submitting sensitive information.

2. Search Engines

A search engine is an online tool that helps users locate information on the Internet by entering keywords or questions.

Examples include Google, Bing, and DuckDuckGo.

Search engines generally discover web pages, index their content, and retrieve relevant results in response to a search query.

How to use a search engine effectively:

- 1 Open a search engine.
- 2 Enter clear and specific keywords.
- 3 Review the search results.
- 4 Open relevant pages.
- 5 Verify information using reliable sources.

For example, searching for digital fluency syllabus PDF is more useful than entering only digital when looking for a particular syllabus.

3. Search Strategies

Search strategies are techniques used to find accurate and relevant information quickly.

- Use specific keywords: Search for the exact topic required.
- Use quotation marks: Search for an exact phrase, such as "digital fluency".
- Use AND: Find results containing both concepts, where the search engine supports this operator.

- Use OR: Find results containing either of two alternatives.
- Use a minus sign: Exclude an unwanted term, such as jaguar -car.
- Search within a website: Use site:example.com topic.
- Check publication dates: Useful when current information is needed.
- Verify sources: Compare information across credible websites.

Effective searching reduces irrelevant results and improves the quality of information collected.

4. Creating and Managing Email Accounts

Email, or electronic mail, is a digital communication system used to send and receive messages and attachments over the Internet.

Examples of email services include Gmail, Outlook, and Yahoo Mail.

Steps to create an email account:

- 1 Visit the official website or application of an email provider.
- 2 Select the account creation option.
- 3 Enter the required details.
- 4 Choose a unique username and a strong password.
- 5 Complete any required verification.
- 6 Review the account's security and recovery settings.

Managing an email account involves organising messages, deleting unwanted emails, creating folders or labels, managing contacts, and checking security settings.

Users should protect their login credentials and enable two-factor authentication where available.

5. Composing and Sending Emails

An email generally contains a recipient, subject, message body, and sender information.

Example:

Respected Sir/Madam,

I am submitting my assignment for your kind consideration. Please find the attached document.

Thank you.

Yours sincerely,

Student Name

Before sending an email, check the recipient's address, subject line, spelling, attachments, and overall tone.

6. Email Etiquette and Best Practices

Email etiquette refers to the rules of polite and professional communication through email.

Important practices:

- Use a clear and meaningful subject line.
- Begin with an appropriate greeting.
- Keep the message concise and relevant.

- Use polite and professional language.
- Avoid writing the entire message in capital letters.
- Check grammar and spelling before sending.
- Attach the correct files and mention them in the message.
- Use Reply All only when everyone needs the response.
- Avoid sharing confidential information unnecessarily.
- Respond to important emails within a reasonable time.

Good email etiquette creates a professional impression and prevents misunderstandings.

7. Introduction to Social Media Platforms

Social media platforms are digital services that allow users to communicate, share content, build communities, and interact with individuals or organisations.

Facebook

Used for connecting with people, creating groups and pages, sharing posts, promoting businesses, and participating in communities.

Instagram

Focuses on photos, videos, Stories, Reels, and visual communication. Businesses use it to display products and reach customers.

YouTube

A video-sharing platform used for education, entertainment, tutorials, live streams, and business promotion.

WhatsApp

Used for instant messaging, voice and video calls, group communication, and sharing documents and media.

LinkedIn

A professional networking platform used for job searches, career development, professional connections, and business networking.

Social media offers opportunities for communication and learning, but users must also consider privacy, misinformation, cyberbullying, and excessive use.

8. Privacy and Security Settings

Privacy settings determine who can view a user's information and content, while security settings help protect the account from unauthorised access.

Important privacy and security practices:

- Keep personal profiles private when appropriate.
- Limit who can see posts, photographs, and contact details.
- Use strong, unique passwords.
- Enable two-factor authentication.
- Review connected applications and account permissions.
- Control location sharing and tagging.
- Block and report suspicious or abusive accounts.
- Review account activity and active login sessions.

Privacy settings reduce unnecessary exposure of personal information, while security measures help prevent account theft and misuse.

9. Creating and Managing Social Media Accounts

Creating a social media account generally involves choosing a platform, registering with an email address or phone number, verifying the account, and setting up a profile.

Account management includes:

- Choosing an appropriate username and profile photograph.
- Writing a suitable biography or description.
- Managing followers, friends, and contacts.
- Creating posts and responding to comments.
- Reviewing privacy and security settings.
- Removing unwanted content and blocking suspicious users.
- Maintaining a positive and responsible online presence.

For business accounts, users should provide accurate business information and maintain consistent communication with customers.

10. Posting and Sharing Content

Posting refers to publishing text, images, videos, links, or other information on a social media platform. Sharing means distributing existing content to other users or audiences.

Types of content:

- Text posts and status updates.
- Photographs and infographics.
- Videos and short-form reels.
- Stories and live broadcasts.
- Links to websites and articles.
- Educational and promotional content.

Best practices for posting:

- 1 Identify the purpose and intended audience.
- 2 Use clear, relevant, and accurate information.
- 3 Choose suitable images or videos.

- 4 Obtain permission before sharing another person's private photographs or information
- 5 Respect copyright and give credit when required.
- 6 Check facts before publishing.
- 7 Avoid sharing sensitive personal details.
- 8 Review the content before posting.

Responsible content sharing helps protect privacy, maintain credibility, and promote positive digital communication.

Online Safety and Cybersecurity

Online safety is included in the course objectives, so it is important to prepare these topics for examinations as well.

1. Meaning of Cybersecurity

Cybersecurity refers to the practices, technologies, and measures used to protect computers, networks, accounts, and digital information from unauthorised access, damage, theft, or misuse. Its main objectives are to protect the confidentiality, integrity, and availability of information.

- Confidentiality: Only authorised people can access information.
- Integrity: Information remains accurate and is not altered improperly.
- Availability: Information and systems remain accessible when required.

2. Common Cybersecurity Threats

Cybersecurity threats are activities or events that can compromise devices, accounts, or information.

Phishing

Fake messages or websites designed to steal sensitive information

Malware

Harmful software that damages systems or steals data

Virus

Malicious code that attaches to files or programs and spreads when executed

Ransomware

Malware that locks or encrypts data and demands payment

Identity theft

Misuse of another person's personal information

Online fraud

Deception used to steal money or obtain benefits

Hacking

Unauthorised access to computer systems or accounts

Cyberbullying

Using digital platforms to harass, threaten, or humiliate others

Users should avoid suspicious links and attachments, install security updates, use reputable security software, and verify requests for money or confidential information.

3. Protecting Personal Information Online

Personal information includes details such as a person's full name, phone number, home address, photographs, passwords, financial details, and identity documents.

Ways to protect personal information:

- Share only necessary information online.
- Never disclose passwords or one-time passwords (OTPs) to others.
- Avoid uploading identity documents on unverified websites.
- Use secure websites for sensitive transactions.
- Avoid sensitive activities on untrusted public Wi-Fi networks.
- Keep devices and applications updated.
- Review app permissions and privacy settings.
- Maintain backups of important files.

Protecting personal information reduces the risk of identity theft, financial fraud, and privacy violations.

4. Password Safety

A password is a secret combination of characters used to authenticate a user's identity.

A strong password should be long, unique, and difficult to guess. Passwords should not contain easily available personal details, such as birthdays or names.

Best practices: Use a different password for every important account, use a password manager when appropriate, enable two-factor authentication, and never share passwords with other people.

5. Safe Online Behaviour

Safe online behaviour means using digital technologies in a responsible manner while protecting oneself and others from online risks.

Important practices include:

- Verify information before forwarding it.
- Avoid clicking unknown links.
- Do not communicate sensitive information through unverified channels.
- Treat other users respectfully.
- Report cyberbullying, fraud, and suspicious activities.
- Respect intellectual property and other people's privacy.
- Log out of accounts on shared devices.
- Download software only from trusted sources.

In India, cybercrime complaints can be reported through the official National Cyber Crime Reporting Portal at cybercrime.gov.in. For immediate financial cyber fraud, contact the national helpline 1930 as soon as possible.

tings on a social media account.