Information Security Policy

This policy sets out how Digital Unite protects information used in its work and ensuring its confidentiality, integrity and availability.

It provides overall direction for information security across the organisation and is supported by more detailed policies and procedures, including the Data Protection Policy, Cybersecurity Policy, Digital Working Policy.

This policy will be reviewed regularly to ensure it remains appropriate in the light of any changes to the law, organisational policies or contractual obligations.

Scope

This policy provides management direction and support for information security across the organisation.

This policy applies to all employees, contractors, volunteers and any individual who has permanent or temporary access to Digital Unite's information, systems, platforms, data or devices.

The policy applies to all forms of information, including:

- Electronic records
- Emails and cloud systems
- Paper files
- Verbal discussions
- Photographs and media

The aim is to ensure information is:

- Kept confidential where necessary
- Accurate and reliable
- Available when needed
- Protected from loss, misuse, unauthorised access, or disclosure

What do we mean by information

The term “information” used in this document refers to knowledge obtained through the course of Digital Unite’s business activities and held in some form (including paper, electronic or other means).

Information should be handled according to its sensitivity.

1. **Public:** Information approved for public sharing, such as published reports or website content.
2. **Internal**: Routine internal information not intended for public distribution.
3. **Confidential**: Sensitive information that could cause harm or distress if disclosed, including Personal data, Safeguarding information, financial records, HR information

Loss of Confidential information could seriously damage Digital Unite’s reputation and lead to financial loss. Confidential information should only be shared with authorised individuals and stored securely.

Information that is not specifically classified as Public should be considered Confidential.

Roles and Responsibilities

Management

Management is responsible for implementing this policy and ensuring staff and volunteers understand their responsibilities.

Staff, Contractors and Volunteers must

- Follow this policy and related procedures
- Keep passwords secure
- Report security incidents or concerns promptly
- Only access information needed for their role
- Handle confidential information responsibly

Information gathered

Information will only be gathered for specific purposes, and in compliance with the General Data Protection Regulations.

In order to respond to requests for information efficiently, the organisation will use effective records management systems and will audit the accuracy of the information held.

Confidential information will not be shared with other parties without contractual obligations in place to maintain its security. Decisions to share information with other parties must be agreed by the designated Digital Unite Data Protection Officer.

Confidential information will not be transported without reasonable precaution.

Data Protection Principles

Digital Unite will comply with the following data protection principles when processing personal information:

- we will process personal information lawfully, fairly and in a transparent manner
- we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes
- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay
- we will keep personal information for no longer than is necessary for the purposes for which the information is processed
- we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage

Access Control

Digital Unite operates a “least privilege” approach to access control. This means that users are granted access only to the systems and data required for their role.

Digital Unite will:

- Use individual user accounts where possible
- Remove access when staff or volunteers leave
- Limit administrator access to authorised individuals
- Use strong passwords and multi-factor authentication where available

Users must not:

- Share passwords
- Access information they are not authorised to use
- Leave devices unlocked when unattended

Device and Remote Working Rules

Devices used for work on behalf of Digital Unite should be kept secure.

All staff and volunteers are required to:

- Ensure that all devices are protected with a password, PIN or biometric security
- Keep devices physically secure and not leave them unattended in unsecured environments
- Install operating system and application updates as soon as they are available
- Use antivirus software and firewall protections where appropriate
- Access company systems only via secure and trusted networks
- Take care when working in public places to prevent unauthorised individuals from viewing screens or overhearing confidential conversations
- Avoid the use of removable media such as USB devices unless explicitly required and approved
- Avoid downloading unauthorised or suspicious software

- Avoid accessing unsafe or suspicious websites
- Avoid access to sensitive systems over unsecured networks (where possible use mobile data rather than public Wi-Fi)
- Leaving devices unattended in cars or other locations

For more information, please see the Digital Working Policy and Cyber Security Policy.

Passwords and Authentication

Passwords should:

- Be strong, unique passwords for all systems and services
- Not be reused across multiple platforms
- Be kept confidential and not shared with others
- Stored in the approved password manager (Keeper)
- Changed immediately if there is any suspicion that they have been compromised

Where possible, multi-factor authentication (MFA) should be enabled for:

- Email accounts
- Cloud storage
- Finance systems
- Administrator accounts

For more information, please see the Cyber Security Policy.

Email security

Email remains one of the most common sources of cyber security threats, including phishing, malware and social engineering attacks.

To mitigate these risks, all users must:

- Exercise caution when receiving unexpected emails, particularly those containing links or attachments

- Verify the identity of the sender before taking action
- Avoid clicking on suspicious links or downloading unknown files
- Be alert to common phishing indicators such as urgency, unusual requests or inconsistencies in the message

If there is any doubt about the legitimacy of an email, it should not be engaged with and must be reported.

Physical Security

Paper records and physical devices containing information must be stored securely.

Digital Unite will:

- Secure storage areas where paper records are held
- Limit access to confidential paper records
- Dispose of confidential waste securely

Staff and volunteers avoid

- printing confidential information where possible
- leaving confidential papers unattended in public or shared spaces.

Data Sharing and Third Parties

Information should only be shared where there is a legitimate reason to do so.

Before sharing confidential or personal information, consideration should be given to:

- Whether sharing is necessary
- Whether consent or another lawful basis applies
- Whether the recipient can protect the information appropriately
- Whether a secure link can be used rather than attaching a file to an email

Third-party providers handling Digital Unite's data should be reputable and use appropriate security measures.

For more information, please see the Data Protection Policy and Cyber Security Policy.

Incident Reporting

All actual or suspected information security incidents must be reported promptly to Emma Weston.

Examples include:

- Lost or stolen devices
- Phishing emails
- Accidental disclosure of information
- Unauthorised access
- Malware or ransomware incidents
- Loss of paper files

Incidents will be assessed and managed appropriately, including consideration of any legal reporting obligations under data protection law.

Backup and Recovery

Important information should be backed up regularly where practical.

Digital Unite will take reasonable steps to ensure important systems and records can be restored in the event of:

- Hardware failure
- Cyber incident
- Accidental deletion
- Other disruption

Critical information should not be stored solely on one device where avoidable.

Training and Awareness

Staff, volunteers, and trustees will receive appropriate awareness of:

- Data protection responsibilities

- Phishing and cyber risks
- Secure handling of information
- Incident reporting procedures

Refresher training or reminders will be provided periodically.

Contact us

If you have any questions, please get in touch: du@digitalunite.com