camara education real impact through technology

CAMARA EDUCATION DATA PROTECTION POLICY (2026 Update)

Reviewed August 2026
Date of next review August 2027

Purpose of this policy

This policy sets out Camara Education's commitment to protecting the rights and privacy of individuals and applies across all Camara Education operations. Camara Education will comply with the General Data Protection Regulation (GDPR) and UK GDPR where applicable, and with all applicable data protection and privacy legislation in each country in which it operates. The principles of the GDPR and UK GDPR set out in this policy provide Camara Education's overarching standard for the responsible handling of personal data.

Responsibility

Personal data means any information relating to an identified or identifiable living individual. Camara Education is responsible for ensuring that personal data under its control is collected, used, stored, shared and disposed of appropriately and securely, in accordance with applicable data protection legislation. All employees, volunteers, consultants and contractors who handle personal data on behalf of Camara Education are responsible for complying with this policy.

For further details, refer to the official sources:

- European Commission – Data Protection and GDPR
- Data Protection Commission (Ireland)
- Information Commissioner's Office (UK) – Data Protection

Principles of Data Protection

Camara Education will apply the following data protection principles across its operations, in accordance with the GDPR and UK GDPR where applicable, and relevant data protection legislation in each country in which it operates:

1. **Lawfulness, Fairness, and Transparency**
   Camara will obtain and process personal data lawfully, fairly, and transparently, ensuring that individuals are aware of how their data is used.
2. **Purpose Limitation**
   Camara will collect personal data only for specified, explicit, and legitimate purposes and will not further process it in a way incompatible with those purposes.

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org

3. **Data Minimisation**
   Personal data collected by Camara will be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
4. **Accuracy**
   Camara will ensure personal data is accurate and, where necessary, kept up to date. Inaccurate data will be rectified or deleted without undue delay.
5. **Storage Limitation**
   Personal data will be retained for no longer than necessary for the purposes for which it was collected, in line with Camara's Data Retention Policy.
6. **Integrity and Confidentiality**
   Camara will ensure personal data is processed securely using appropriate technical and organisational measures, protecting it from unauthorised or unlawful processing, accidental loss, destruction, or damage.
7. **Accountability**
   Camara acknowledges its responsibility for ensuring compliance with applicable data protection legislation and will demonstrate this compliance through policies, procedures, and appropriate documentation.

Personal Data

Definition
Personal data means any information relating to an identified or identifiable living individual.

Data Protection
Camara Education is committed to protecting personal data from unauthorised access, use, disclosure, alteration, loss or destruction during processing and storage.

Electronic Data Security
All personal electronic data must be protected by appropriate security controls, which may include:

- **Password protection**
- **Encryption**
- **Access controls and logs**
- **Regular backups**

Visibility and Access

- Screens, printouts, documents and files containing personal data must not be visible or accessible to unauthorised individuals.
- Personal data held in physical form must be stored securely in locked cabinets, locked rooms

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org

or areas with restricted access.

Retention and Disposal

Personal data will be retained only for as long as necessary for the purposes for which it was collected and in accordance with Camara Education's Data Retention Policy and applicable data protection legislation. Physical records containing personal data must be securely destroyed when the applicable retention period has expired.

Hardware Management

When upgrading, replacing, disposing of or transferring computers or other data-bearing equipment, Camara Education must ensure that any stored data is securely erased or the storage media appropriately sanitised before disposal or reuse.

Donor Equipment Management

Where donor equipment may contain data, Camara Education will use approved IT asset disposition partners and appropriate processes to ensure that data is securely erased and equipment is handled appropriately. Where third-party IT asset disposition partners, including Vyta, are used, appropriate information may be provided to facilitate equipment collection and Camara will retain relevant collection, data erasure and/or asset disposition records where applicable.

Device Security

Special care must be taken when staff laptops and other devices containing personal data are used outside Camara Education premises. Appropriate security measures, including password protection, access controls and encryption where appropriate, must be in place.

Data Controller Responsibilities

Organisations donating devices containing their own data remain responsible for that data until it has been appropriately transferred and/or securely erased in accordance with the agreed process and applicable law. Approved third-party service providers engaged to process or securely erase data must handle that data in accordance with contractual requirements and applicable data protection legislation.

Camara Education's Responsibilities

Where Camara Education determines the purposes and means of processing personal data, including employee, donor and other organisational personal data, Camara Education acts as the data controller or equivalent under applicable law and is responsible for ensuring that the data is handled in accordance with applicable data protection legislation.

Personal data must not be retained for longer than is necessary for the purposes for which it was collected. Camara Education will apply this principle across its operations in accordance with the GDPR where applicable, relevant local data protection legislation and Camara Education's Data Retention Policy.

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org

Retention of Personal Data

Camara Education operates across a number of jurisdictions and is committed to complying with applicable data protection legislation in each country in which it operates. This includes the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 in Ireland, the UK GDPR and Data Protection Act 2018 in the United Kingdom, and applicable national data protection and privacy legislation in the countries in which Camara Education's African hubs operate.

In line with the principle of storage limitation under Article 5(1)(e) of the GDPR and UK GDPR, personal data must not be retained for longer than is necessary for the purposes for which it was collected or processed. Camara Education follows its Documentation Retention Policy and Schedule to ensure that personal data is retained only for as long as required for legitimate organisational purposes or to meet legal, regulatory or contractual obligations.

Personal data that is no longer required will be securely deleted, destroyed or anonymised, as appropriate, in accordance with applicable legislation and Camara Education's data retention and security procedures.

Computer/Password Encryption

Computers and devices used by Camara Education staff and volunteers to access or store personal data must have appropriate security measures in place. These include password protection, access controls and encryption where appropriate, having regard to the nature and sensitivity of the personal data being processed.

Domain and Account Security

Camara Education uses Google Workspace for Nonprofits to manage organisational email accounts and collaboration tools for staff and volunteers.

- **Email Account Creation:** Email accounts are created in accordance with Camara Education's applicable HR and IT procedures. New users are provided with secure access credentials and are required to change temporary passwords where applicable.
- **Camara Email Accounts:** Organisational email accounts and approved Camara domains and aliases are centrally managed by Camara Education.
- **Two-Factor Authentication (2FA):** Two-factor authentication is required for organisational accounts where supported and mandated by Camara Education's IT security procedures.
- **Device Security:** Appropriate antivirus, security and endpoint protection must be maintained on devices used to access or process Camara Education data, where applicable.
- **Password Security:** Passwords must comply with Camara Education's IT security requirements and applicable platform security standards. Users are responsible for creating strong passwords and keeping their login credentials confidential.

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org

- **Password Recovery:** Users who forget or are locked out of their passwords should contact the relevant IT/System Administrator for account recovery and support.
- **Account Management:** Accounts provided to staff and volunteers remain active only for as long as required for their role or placement. Account holders are responsible for maintaining the security of their accounts and complying with Camara Education's IT and data security requirements.
- **Termination of Accounts:** When an employee, contractor or volunteer leaves Camara Education or no longer requires access, organisational accounts and access permissions will be deactivated, removed or otherwise managed in accordance with Camara Education's HR and IT procedures.

Dublin Active Directory Policy 2026

Camara Education uses a Windows-based Active Directory (AD) environment in its Dublin operations to securely manage and administer user accounts and devices.

- All personnel using the Dublin Active Directory environment use Windows 11 machines.
- Active Directory services are managed through Windows Server 2022, with the following key services enabled:
    - **Active Directory Domain Services:** Used for user account creation and management, computer management and the enforcement of domain-applied settings.
    - **DNS Server:** Supports network connectivity and the management of access to online resources.
    - **File Services:** Facilitates secure file sharing between authorised users and provides access to relevant application databases.
    - **Print and Document Services:** Ensures authorised office network printers and related document services are available to users.
    - **Group Policy:** Enforces domain-wide settings on computers, including:
        - **Power Settings:** Screens switch off after 10 minutes of inactivity, computers enter sleep mode after 15 minutes and enter hibernate mode after 1 hour.
        - **Application Control:** Installation of new software is restricted through Windows User Account Control and applicable administrative permissions. Only IT-approved or trusted software may be installed on user devices.
- **Password Strength Policy:** Passwords must meet the security requirements applied to the domain and Camara Education's current IT security requirements, including appropriate password length and complexity.
- **Password Recovery:** Recovery of forgotten or locked passwords is managed by the IT team. Users must contact IT for assistance with password recovery.

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org

Dublin Internet Security Policy 2026

Camara Education uses internet and endpoint security software on Dublin domain computers to help protect organisational data and systems against cyber threats. The current security solution is Norton, which provides security functions including:

- **Anti-Virus**
  Detects and protects against malware, including viruses, ransomware and other malicious software.
- **Anti-Spyware**
  Helps prevent spyware and other malicious applications from compromising computers or organisational data.
- **Safe Surfing**
  Helps protect users against malicious websites, phishing attempts and fraudulent sites.
- **Intrusion Prevention**
  Helps identify and block network threats and suspicious activity that could compromise systems.
- **Email and Online Threat Protection**
  Helps protect users against malicious links, downloads, phishing attempts and other online threats.
- **Firewall Protection**
  Monitors and controls network traffic to help protect against unauthorised access and potential threats.

Threat Response

Where a threat is detected, the security software may automatically block or quarantine the affected file or activity. When an alert is generated, the IT team will review the incident and take appropriate action, which may include removing quarantined items and carrying out further system scans or investigation.

Camara Education's IT team is responsible for maintaining and updating the relevant security systems to provide appropriate protection against evolving cyber threats.

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org

Firewall and Cloud Security Policy 2026

Camara's Cloud-Based Security Measures

- Camara Education makes extensive use of cloud-based services, including Google Workspace, Google Docs and Google Drive, to support its operations, communications and storage of organisational data. Appropriate security controls are maintained across Camara's cloud-based systems and IT infrastructure.
- Cloud Security and Threat Detection
  Google Workspace provides security features including data encryption, two-factor authentication (2FA), access controls, phishing detection and malware protection. Camara uses appropriate available security controls to help prevent unauthorised access and mitigate cyber threats.
- Access Control and Data Encryption
  Data stored within Google Workspace is protected by Google's security and encryption measures. Camara applies access controls to ensure that sensitive organisational information is accessible only to authorised personnel according to their roles and responsibilities.
- Remote Access and Device Security
  Devices used to access Camara Education systems and data must have appropriate security measures in place. Access to sensitive information is restricted to authorised users, and staff and volunteers are responsible for complying with Camara's IT and data security requirements when working remotely.
- Ongoing Security Monitoring and Updates
  Camara Education regularly reviews its IT and cloud security arrangements and applies appropriate security updates and controls to protect against emerging threats. The IT team is responsible for overseeing relevant systems and responding to identified security issues.

Customer Relationship Management (CRM) Policy 2026

Camara Education no longer operates a dedicated CRM system for day-to-day customer and donor management. Organisational information is managed through approved Camara systems in accordance with this Data Protection Policy and applicable data protection legislation.

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org

Historical Salesforce Data

- Salesforce is retained for limited access to historical records, including legacy customer, inventory and shipment information.
- Salesforce is not used as Camara Education's primary CRM system and is accessed only when historical information is required for legitimate organisational purposes.
- Access is restricted to authorised personnel and appropriate account security measures, including two-factor authentication (2FA), are maintained.
- Historical personal data held within Salesforce is subject to Camara Education's Documentation Retention Policy and Schedule and should not be retained for longer than necessary.

Security Measures

Access to systems containing customer, donor or other personal information is restricted to authorised personnel. Appropriate access controls and security measures must be maintained in accordance with Camara Education's IT security requirements and applicable data protection legislation.

Google Workspace Policy 2026

Google Workspace is Camara Education's principal cloud-based platform for organisational email, file sharing, document collaboration, meetings and calendar management.

- **Email Accounts:** Camara Education provides authorised users with organisational email accounts using approved Camara domains and aliases.
- **Two-Factor Authentication (2FA):** Two-factor authentication is required for organisational accounts in accordance with Camara Education's IT security requirements.
- **Google Drive:** Organisational files may be stored and shared through Google Drive. Access permissions must be appropriately managed so that confidential or personal information is accessible only to authorised users.
- **Encryption and Security:** Data stored and transmitted through Google Workspace is protected by Google's security and encryption measures. Camara Education maintains appropriate account and access controls to protect organisational information.
- **Customer and Donor Communication:** Customer, donor and partner communications involving Camara Education business should be conducted through authorised Camara Education accounts and systems where appropriate.

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org

Security of Personal Data

Camara Education will take appropriate technical and organisational measures to ensure the security of personal data, in accordance with Article 32 of the GDPR and UK GDPR where applicable, and relevant data protection legislation in each country in which it operates. These measures include:

1. **Encryption and Device Security:** Appropriate encryption and security measures will be used to protect personal electronic data, taking account of the nature and sensitivity of the data and the systems or devices on which it is stored.
2. **Access Controls:** Access controls will be maintained to ensure that only authorised personnel have access to personal data.
3. **Data Anonymisation and Pseudonymisation:** Where appropriate, personal data will be anonymised or pseudonymised to protect the identity of individuals.
4. **Security Reviews:** Security measures and risks will be reviewed periodically to ensure that personal data remains appropriately protected.

Retention of Personal Data

Camara Education will retain personal data only for as long as necessary for the purposes for which it was collected or as required by applicable legal, regulatory or contractual obligations. Retention will be managed in accordance with Camara Education's Documentation Retention Policy and Schedule, the storage limitation principle under the GDPR and UK GDPR where applicable, and relevant local data protection legislation.

Personal data that is no longer required will be securely deleted, destroyed or anonymised, as appropriate. Physical records containing personal data will be securely destroyed.

Data Breach Notification

Camara Education will respond promptly to any actual or suspected personal data breach in accordance with its Data Breach Policy and Procedures and applicable data protection legislation.

Where the GDPR applies, Camara Education will notify the relevant supervisory authority of a reportable personal data breach without undue delay and, where feasible, within 72 hours of becoming aware of it, as required by Article 33 of the GDPR. Where UK GDPR applies, Camara Education will follow the corresponding UK requirements and notify the UK Information Commissioner's Office (ICO) where required.

For operations in other jurisdictions, Camara Education will comply with applicable local requirements for reporting personal data breaches to the relevant authority and/or affected individuals.

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org

Where required by applicable law, individuals affected by a personal data breach will also be informed without undue delay.

Data Processors

Camara Education will ensure that third-party service providers processing personal data on its behalf are subject to appropriate contractual, confidentiality and data protection requirements. Where required by applicable law, appropriate Data Processing Agreements (DPAs) will be put in place.

Third-Party and International Data Transfers

Where personal data is transferred internationally, including between Camara Education entities or to third-party service providers, Camara Education will ensure that appropriate safeguards are in place as required by applicable data protection legislation.

For transfers subject to the GDPR or UK GDPR, this may include applicable adequacy decisions, Standard Contractual Clauses, the UK International Data Transfer Agreement or other legally recognised transfer mechanisms, as appropriate.

Updates to Policies and Procedures

Camara Education will regularly review and update its data protection policies and procedures to reflect applicable data protection legislation in the jurisdictions in which it operates. Staff and relevant volunteers will receive appropriate data protection guidance or training, and appropriate documentation will be maintained to support and demonstrate compliance.

Camara Education
40A Sandymount Avenue,
Dublin 4, Ireland
Website: camara.org
Email : info@camara.org