camara education real impact through technology

CAMARA EDUCATION DATA PROTECTION POLICY (2024 Update)

Reviewed October 2024
Date of next review October 2025

Purpose of this policy

This policy is a statement of Camara Education's commitment to protect the rights and privacy of individuals in compliance with the General Data Protection Regulation (GDPR) 2018, the Data Protection Act 2018, Data Protection Act 1988, the Data Protection (Amendment) Act 2003 and subsequent regulations up to 2024.

Responsibility

Under the Data Protection Acts, "personal data" is defined as data relating to a living individual who is or can be identified from that data, or from the data combined with other information that is in, or likely to come into the possession of, the data controller (Data Protection Act 1988, Section 1). Data protection is essential for safeguarding the privacy of individuals concerning the processing of their personal data. The Data Protection Acts of 1988 and 2003 confer rights upon individuals while placing responsibilities on those processing personal data.

For further details, refer to the official sources:

- Data Protection Commission (Ireland) - What is Personal Data?
- UK Information Commissioner's Office - Guide to Data Protection

The General Data Protection Regulation (GDPR), effective as of May 25, 2018, along with the Irish Data Protection Act 2018, defines "personal data" as any information relating to an identified or identifiable living individual (data subject). An identifiable person is one who can be identified, directly or indirectly, through identifiers such as name, ID number, location data, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

The GDPR enforces the principles of data protection, safeguarding individuals' privacy concerning the processing of their personal data. It confers specific rights on individuals and places enhanced obligations on data controllers and processors.

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

Principles of the GDPR

Camara will adhere to its responsibilities under the GDPR in accordance with the following principles:

1. **Lawfulness, Fairness, and Transparency**
   Camara will obtain and process personal data lawfully, fairly, and transparently, ensuring that data subjects 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.
3. **Data Minimisation**
   Personal data collected by Camara will be adequate, relevant, and limited to what is necessary in relation to 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 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 or organisational measures, protecting it from unauthorised or unlawful processing, accidental loss, destruction, or damage.
7. **Accountability**
   Camara acknowledges its responsibility for ensuring compliance with the GDPR and will demonstrate this compliance through policies, procedures, and appropriate documentation.

Principles of Data Protection (GDPR)

Camara will administer its responsibilities under the General Data Protection Regulation (GDPR) in accordance with the seven key data protection principles outlined in Article 5 of the GDPR, as follows:

1. Lawfulness, fairness, and transparency- Camara will obtain and process personal data lawfully, fairly, and in a transparent manner. Individuals will be informed about how their personal data is being used and for what purposes.

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

2. Purpose limitation- Camara will collect personal data only for specified, explicit, and legitimate purposes. Data will not be processed further in any manner incompatible with those purposes unless explicit consent is obtained or processing is required by law.

3. Data minimisation- Camara will ensure that personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

4. Accuracy- Camara will take all reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date. Inaccurate data will be rectified or erased without delay.

5. Storage limitation- Camara will retain personal data only for as long as is necessary for the purposes for which it was collected and processed, in line with Camara's Data Retention Policy. After this period, the data will be securely deleted or anonymised.
6. Integrity and confidentiality (security)

Camara will implement appropriate technical and organisational measures to ensure the security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

7. Accountability- Camara will ensure compliance with these principles and be able to demonstrate accountability. Procedures will be in place to document data processing activities and to ensure that data subjects' rights are respected.

8. Rights of Individuals (Data Subjects) Camara will ensure that data subjects can exercise their rights under the GDPR, including but not limited to:

- Right of access: Individuals can request a copy of their personal data.
- Right to rectification: Individuals can request correction of inaccurate or incomplete data.
- Right to erasure ("right to be forgotten"): In certain circumstances, individuals can request the deletion of their personal data.
- Right to data portability: Individuals can request their data in a structured, commonly used format.
- Right to object and restrict processing: In certain situations, individuals can object to or request the restriction of data processing.

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

Personal Data

Definition
Personal data is defined as: "data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of the data controller" (Source: Data Protection Commission, What is Personal Data?).

Data Protection
Camara is committed to protecting personal data from unauthorised access during processing and storage, as well as safeguarding it from inadvertent destruction, alteration, or corruption.

Electronic Data Security
All personal electronic data is subject to stringent security controls, including:

- **Password protection**
- **Encryption** (using appropriate standards such as AES)
- **Access logs**
- **Regular backups**

Visibility and Access

- Screens, printouts, documents, and files containing personal data must not be visible to unauthorised individuals.
- Personal manual data must be stored securely in locked cabinets, locked rooms, or areas with restricted access.

Retention and Disposal
In line with our data retention policy, personal manual data will be destroyed through confidential shredding once the retention period has expired.

Hardware Management
When upgrading or replacing computers, the IT person must ensure that the hard drives are properly sanitised.

Donor Equipment Management
Donor equipment is collected by Vyta and stored at their facility. Camara provides Vyta with the necessary donor information to facilitate equipment collection. Vyta will then send Camara a Collected Items Report (CIR) and an Asset Settlement Report detailing the final disposition of all donated equipment.

Device Security
Special care must be taken when staff laptops and devices containing personal data are used

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

outside the organisation. These devices must have encryption and appropriate security measures in place.

Data Controller Responsibilities

Organisations that donate devices containing data on hard drives retain their responsibility as data controllers. Vyta acts as a third-party data processor, responsible for securely wiping data on behalf of Camara.

Data Controller Identification

In matters involving Camara's personal data—such as employee information (including PPS numbers, bank account details, etc.) and aggregated personal donor data (like mailing lists)—Camara operates as the data controller and is responsible for ensuring compliance with all relevant data protection legislation.

Under the Data Protection Acts 1988 and 2003 in Ireland, data controllers were required to adhere to section 2(1)(c)(iv) of the Acts, which mandated that "the data shall not be kept for longer than is necessary for that purpose or those purposes."

Since the introduction of the General Data Protection Regulation (GDPR) in 2018, data retention is now regulated by Article 5(1)(e) of the GDPR. This article sets the standard for storage limitation, stipulating:

> "Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."

In line with Irish and EU law in 2024, Camara ensures that data retention policies reflect Article 5(1)(e) of the GDPR rather than section 2(1)(c)(iv) of the older Data Protection Acts. This policy update guarantees that all personal data is retained only as long as necessary for the intended purposes, maintaining Camara's full compliance with current data protection regulations.

Retention of Personal Data

In line with Article 5(1)(e) of the General Data Protection Regulation (GDPR), personal data shall not be retained for longer than is necessary for the purposes for which it was collected or processed. Camara Education is committed to adhering to this principle by following the Camara Education Documentation Retention Policy and Schedule. This policy includes regular audits and reviews to ensure that personal data is either anonymised or securely deleted once it is no longer required for the legitimate business purposes or legal obligations it was originally collected for.

Data that is no longer needed will be securely deleted or anonymised in accordance with best

practices and GDPR guidelines to prevent unauthorised access or misuse.

Computer/Password Encryption

All computers used by Camara Education staff and volunteers are encrypted to meet GDPR's security requirements for safeguarding personal data.

Domain Policy 2024

Camara uses a domain based on Google Workspace for Nonprofits to manage email accounts and collaboration tools for staff and volunteers.

- Email Account Creation:
  All email accounts are created in accordance with the Camara Email Procedure document, which can be found in the CEL HR Policy documents. When a new email account is created, users are provided with a temporary password by the IT System Admin and are prompted to change this password upon their first login.
- All user accounts are set up with the @camara.ie domain, and the @camara.org alias is also active for all users.
- Two-Factor Authentication (2FA): Mandatory for all accounts, ensuring secure access. Users must authenticate using a secondary verification method to enhance account security.
- Norton AntiVirus: The accounts team is protected with Norton AntiVirus software to provide additional layers of security.
- Password Strength Policy:
  The password strength policy for the domain requires:
  - A minimum of 8 characters (alphanumeric).
  - The use of upper and lower case letters, numbers, and special characters.
  - A password strength indicator is enabled to guide users in setting a strong password.
- Passwords must comply with Google Workspace's security standards, including periodic reminders to change weak passwords.
- Password Recovery:
  Users who forget or lock their passwords can contact the IT System Admin for password recovery and account support.
- Account Management: Google Workspace accounts created for staff and volunteers remain active for the full length of their contract or placement. Each account holder is responsible for maintaining the security of their account by adhering to Camara IT's security policies and following Google's security best practices, which can be accessed on the Google Security Recommendations page.
- Termination of Accounts:
  Upon contract termination or the end of a volunteer placement, Google Workspace and

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

Active Directory accounts are deactivated or deleted as per the termination policy outlined in the Camara HR and IT procedures.

Dublin Active Directory Policy 2024

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

- All personnel now use Windows 11 machines.
- Active Directory services are managed by Windows Server 2022, with the following key services enabled:
    - Active Directory Domain Services: This service is used for user account management and creation, computer management, and the enforcement of domain-applied settings with various applications.
    - DNS Server: This service manages external network connectivity and filtering, ensuring users are blocked from accessing websites that may pose risks to the Camara network.
    - File Services: This service facilitates secure file sharing between users and provides access to an application database.
    - Print and Document Services: This service ensures all office network printers are available to users and supports office-wide document management.
    - Group Policy: This service enforces domain-wide settings on all computers, including:
        - Power Settings: The following power-saving configurations apply across all user machines: 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 under Windows User Account Control for security reasons. Only IT-approved or trusted software can be installed on user devices.
- Password Strength Policy: The password strength policy for the domain now requires:
    - A minimum of 8 characters (previously 6).
    - Upper and lower case letters, numbers, and special characters
- Password Recovery: Recovery of forgotten or locked passwords continues to be managed solely by the IT department. Users must contact IT for assistance with password recovery.

Internet Security Policy 2024

Camara uses **i**ndustry-standard internet security software on all domain computers to ensure data protection and prevent cyber threats. The current security solution in place is NortonLifeLock (formerly Symantec Endpoint Protection), which provides comprehensive protection including:

- **Anti-Virus**
  Detects and removes malware, including viruses, ransomware, and other malicious software.
- **Anti-Spyware**
  Prevents spyware from infiltrating computers and protects user data from being tracked or stolen.
- **Safe Surfing**
  Protects users from malicious websites, phishing attacks, and fraudulent sites while browsing the internet.
- **Intrusion Prevention**
  Blocks potential network threats and suspicious activity that could compromise the network's integrity.
- **Email Protection**
  Scans all incoming and outgoing emails for malware, phishing attempts, and harmful attachments to safeguard communication channels.
- **Smart Firewall**
  Monitors and controls inbound and outbound network traffic to protect against unauthorised access and potential threats.

Threat Response:
If any threats are detected, Norton automatically blocks the threat, either by preventing the suspicious file or package from entering the computer or by quarantining the affected file. An automatic alert is sent to the IT team, who then reviews and removes any quarantined items and performs a full system scan on the affected computer to ensure the system's integrity.

Camara's IT team monitors and regularly updates the security software to ensure optimal protection against evolving cyber threats.

Firewall Policy 2024
Camara's Cloud-Based Security Measures

- At Camara, we operate fully in the cloud, utilising Google Workspace, which includes Google Docs, Google Drive, and other collaboration tools to manage our operations and store critical data. While we do not have a physical office or rely on on-site servers, we ensure data security and network protection through the robust security features provided by Google Workspace.
- Cloud Security and Threat Detection
  Google Workspace offers comprehensive cloud security, including data encryption, two-factor authentication (2FA), and access control, ensuring that all data remains secure. We also utilise Google's built-in security measures like phishing detection and malware protection to prevent unauthorised access and mitigate cyber threats.
- Access Control and Data Encryption
  All documents, communications, and data stored within Google Workspace are encrypted

both in transit and at rest. We enforce strict access controls, limiting access to sensitive information only to authorised personnel, ensuring security and compliance.

- Remote Access and Device Management
  To secure remote work, we implement Google Workspace's device management tools, which allow us to monitor, manage, and secure all devices accessing our cloud environment. This includes ensuring that only trusted devices can access sensitive files, providing a secure working environment for all team members, regardless of location.
- Ongoing Security Monitoring and Updates
  We regularly review and update our security settings in Google Workspace, making use of the latest updates and best practices to protect against emerging threats. Our IT person continuously monitors the system to ensure that our data and communications remain secure.

Customer Relationship Management (CRM) Policy 2024

Camara now utilises HubSpot as its primary CRM system for managing customer, donor, staff, and volunteer information, while Salesforce continues to be used for specific operational needs.

HubSpot

- HubSpot is used as Camara's primary CRM tool for managing customer and donor relationships across Dublin and London. It centralises communications and interactions, ensuring a streamlined approach to donor and partner management.
- HubSpot stores essential information, including contact details, communication history, and engagement metrics. It helps to track interactions with customers, donors, staff, and volunteers.
- Inventory management and shipment information are now integrated into HubSpot to improve the visibility of operations. Users have restricted access, ensuring they can only view and edit records necessary for their roles. This is managed through role-based access controls within HubSpot.

Salesforce

- Salesforce is only used for specific functions such as legacy customer records, historic inventory tracking, and past shipment management.
- Sage Financials no longer remains integrated within Salesforce to manage Camara's financial data. Only the Finance team has access to this sensitive financial information.
- Salesforce is secured by two-factor authentication (2FA), using either the Salesforce Authenticator app or Authy. Only authorised personnel have access to the system.

Security Measures

- Two-Factor Authentication (2FA) is mandatory for all CRM users in both HubSpot and historical Salesforce data to ensure data security and prevent unauthorised access.

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

- Access to both systems is role-based, meaning users only have access to the records and tools necessary for their specific roles, ensuring compliance with data protection regulations.

This shift to HubSpot reflects Camara's commitment to leveraging the latest technologies to improve efficiency and collaboration while continuing to rely on Salesforce for specialised historical data.

Google Workspace (formerly GSuite) Policy 2024

Google Workspace is the cloud computing solution used by Camara for email, file sharing, meetings, and calendar management.

- Email Accounts: All user accounts are set up with the @camara.ie domain, and the @camara.org alias is also active for all users.
- Two-Factor Authentication (2FA): Mandatory for all accounts, ensuring secure access. Users must authenticate using a secondary verification method to enhance account security.
- Google Drive: All files are stored and shared via Google Drive. Access to files is managed through strict permissions to ensure only authorised users can view, edit, or share documents.
- Encryption & Security:
    - All data stored within Google Workspace is protected using 128-bit AES encryption.
    - Data in transit between Google and users is encrypted using HTTPS, ensuring secure transmission.
- Customer and Donor Communication: All communication with customers and donors is carried out through Camara's official email accounts, ensuring professionalism and data integrity.

Security of Personal Data

Camara will take appropriate technical and organisational measures to ensure the security of personal data, in compliance with Article 32 of the GDPR. These measures include:

1. Encryption of personal data: All personal electronic data, including on laptops and cloud systems, will be encrypted.
2. Access Controls: Strict access controls will be enforced, ensuring only authorised personnel have access to personal data.
3. Data Anonymisation and Pseudonymisation: Where appropriate, personal data will be anonymized or pseudonymised to protect the identity of individuals.
4. Regular Security Audits: Regular reviews of security measures and risk assessments will be conducted to ensure data is adequately protected.

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

Retention of Personal Data

Camara will retain personal data only for as long as necessary for the purposes for which it was collected. This will be done in line with Camara's Data Retention Policy, ensuring compliance with Article 5(1)(e) of the GDPR.

Personal data that is no longer required will be securely deleted or anonymised, and manual data will be shredded using confidential shredding services.

Data Breach Notification

In line with Article 33 of the GDPR, Camara will notify the Irish Data Protection Commission (DPC) of a personal data breach without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Where the breach is likely to result in a high risk to the rights and freedoms of individuals, Camara will also communicate the breach to the data subjects without undue delay.

Camara has a Data Breach Policy and accompanying Data Breach Procedures in place to handle incidents efficiently and minimise risks.

Data Processors

Camara acknowledges its responsibilities under the GDPR when using third-party processors. All processors engaged by Camara, such as AMI (the third-party responsible for wiping donated equipment), will be required to enter into a Data Processing Agreement (DPA) ensuring that they process data in compliance with the GDPR.

Third-Party Data Transfers

If personal data is transferred outside the European Economic Area (EEA), such transfers will only take place with adequate safeguards in place, as required under Chapter V of the GDPR. This includes the use of Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or adequacy decisions approved by the European Commission.

Updates to Policies and Procedures

Camara will regularly review and update its policies and procedures to ensure ongoing compliance with GDPR and Irish data protection regulations. Staff will receive regular training on data protection obligations, and appropriate documentation will be maintained to demonstrate compliance.

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