9. Information and Data Management

ELI Schools
elischools.com

ELI ENGLISH LANGUAGE INSTITUTE

9. Information and Data Management

Introduction

Effective information and data management is fundamental to quality assurance at ELI Schools. Quality decision-making depends on accurate, timely, accessible information. Student records, assessment data, quality assurance data, financial information, and operational data must be systematically collected, stored, analysed, and used. Furthermore, as an educational institution processing substantial personal data, ELI Schools has significant legal obligations under data protection law (GDPR). This section establishes ELI Schools' approach to information and data management, articulating our information governance framework, data protection policies, and systems for managing institutional information.

Purpose and Scope

The purpose of this section is to:

- Establish ELI Schools' approach to information and data management
- Ensure systematic collection, storage, analysis, and use of information
- Ensure compliance with data protection law (GDPR and Data Protection Act 2018)
- Protect personal data of students, staff, and other data subjects
- Define responsibilities for information and data management
- Establish information security and confidentiality standards

This section addresses:

ELI Schools' approach to information and data management is informed by and complies with:

- Data Protection Act 2018 and General Data Protection Regulation (GDPR):
- QQI Core Statutory Quality Assurance Guidelines 2016
- Code of Practice for Provision of Programmes of English Language Education to International Learners

ELI Schools' Information and Data Management Philosophy

Core Beliefs:

ELI Schools' approach to information and data management is founded on the following core beliefs:

Information Enables Quality:

- Quality decision-making depends on good information
- Systematic collection and analysis of data enable evidence-based improvement
- Information is asset that must be managed effectively

Privacy is Fundamental Right:

- Students and staff have right to privacy
- Personal data must be protected
- Trust depends on respecting privacy and handling data responsibly

Compliance is Non-Negotiable:

- Legal obligations for data protection must be met
- Non-compliance risks significant legal, financial, and reputational consequences
- Compliance is ethical responsibility, not just legal requirement

Security and Confidentiality:

- Information must be secure (protected from unauthorized access, loss, damage)
- Confidential information must remain confidential
- Breaches can cause serious harm to individuals
- Robust security measures essential

Transparency and Accountability:

- Transparent about what data we collect, why, how we use it
- Individuals informed and empowered (data subject rights)
- Accountable for data processing
- Documentation and audit trails

Data Minimization:

- Only collect and retain data that is necessary
- Avoid excessive data collection
- Delete data when no longer needed
- Respect for privacy means not collecting or keeping more than necessary

Accessibility and Usability:

- Information accessible to those who need it (within appropriate access controls)
- Information organized and usable
- Systems and processes enable efficient information retrieval and use

Integration:

- Information management integrated with all operations
- Not separate "data management" function but embedded in everything
- Quality assurance, teaching, student services, operations all depend on information

Types of Information and Data at ELI Schools

ELI Schools collects, processes, and stores various types of information and data:

Student Personal Data:

- Contact details (name, address, email, phone, nationality, passport number, date of birth)
- Demographic data (age, gender, nationality, language)
- Academic records (programme enrolled, level, attendance, assessment results, progression, certificates)
- Financial data (fees paid, payment methods, invoices)
- Accommodation data (host family, address, arrangement details)
- Support data (extenuating circumstances, reasonable accommodations, welfare concerns, complaints)
- Immigration data (visa status, GNIB registration, visa letters issued)
- Medical data (if disclosed - disabilities, health conditions requiring support or extenuating circumstances)
- Safeguarding data (if child safeguarding concerns - highly sensitive)
- Communications (emails, correspondence)
- Images (photographs, videos if student photographed/filmed in classes or activities)

Staff Personal Data:

- Contact details (name, address, email, phone)
- Employment data (role, salary, contract, start date, employment history)
- Qualifications (certificates, transcripts, Garda vetting)
- Performance data (teaching observations, appraisals, CPD)
- Payroll data (bank details, tax information, PRSI)
- Medical data (if disclosed - sick leave, occupational health, reasonable accommodations)
- Disciplinary or grievance data (if applicable)
- Communications

Quality Assurance Data:

- Student feedback (course reviews - anonymous but still data)
- Staff feedback (anonymous)
- Teaching observation reports
- Programme review reports
- Assessment data (aggregated pass rates, grade distributions)
- Complaints and appeals records
- Accreditation and inspection reports

Operational Data:

- Enrolment data (numbers, demographics, trends)
- Financial data (income, expenditure, budgets)
- Accommodation data (host families, capacity, availability)
- Timetabling and scheduling
- Resource data (classrooms, equipment, materials)

Communications and Correspondence:

- Emails (with students, staff, agents, partners, authorities)
- Letters, forms, contracts
- Website content, marketing materials
- Social media

Safeguarding and Safety Data:

- Child safeguarding records (concerns, reports, investigations - highly sensitive)
- Incident reports (accidents, safety incidents)
- Risk assessments
- Health and safety records

Legal and Compliance Data:

- Contracts (with students, staff, suppliers, partners)
- Policies and procedures
- Legal correspondence
- Compliance records (insurance, registrations, licenses)

Intellectual Property:

- Programme materials (syllabi, textbooks, handouts, assessments)
- ELI Schools proprietary materials
- Learning resources

Data Protection Principles (GDPR)

ELI Schools processes all personal data in accordance with GDPR principles:

Lawfulness, Fairness, and Transparency:

- Personal data processed lawfully (legal basis identified)
- Processed fairly (not in ways individuals wouldn't reasonably expect or causing unjustified harm)
- Transparent (individuals informed about data processing through privacy notices)

Purpose Limitation:

- Personal data collected for specified, explicit, legitimate purposes
- Not further processed in ways incompatible with those purposes
- Example: Student data collected for education and administration, not used for unrelated purposes

Data Minimization:

- Only personal data that is adequate, relevant, and necessary is collected
- Avoid collecting excessive data
- Example: Collect student contact details and academic data necessary for education; don't collect irrelevant personal information

Accuracy:

- Personal data is accurate and kept up to date
- Reasonable steps taken to ensure accuracy
- Inaccurate data corrected or erased promptly
- Example: Students can update contact details; errors in records corrected

Storage Limitation:

- Personal data kept only as long as necessary for purposes
- Data retention periods defined
- Data securely deleted when no longer needed
- Example: Student records retained 7 years after completion for transcript verification, then securely destroyed

Integrity and Confidentiality (Security):

- Personal data processed securely
- Protected against unauthorized or unlawful processing, accidental loss, destruction, damage
- Appropriate technical and organizational measures (encryption, access controls, backups, staff training, etc.)

Accountability:

- ELI Schools is responsible for and must demonstrate compliance
- Documentation, policies, records of processing, data protection impact assessments, training, etc.
- Accountability to Data Protection Commission

ELI Schools may process special category data in following situations:

Explicit Consent

- Individual gives explicit consent for specific purpose
- Example: Student explicitly consents to disclosing disability for reasonable accommodations

Employment, Social Security, and Social Protection

- Processing necessary for employment, social security, social protection obligations
- Example: Staff medical data for sick leave, occupational health

Vital Interests

- Necessary to protect life when individual unable to consent
- Example: Medical emergency

Substantial Public Interest

- Processing necessary for reasons of substantial public interest on basis of law
- Example: Processing safeguarding data necessary for child protection (substantial public interest, legal basis in Children First Act)

ELI Schools minimizes processing of special category data, but where necessary (disabilities, medical circumstances, safeguarding), processes lawfully under appropriate GDPR Article 9 basis.

Data Subject Rights

Individuals (students, staff, others) have rights under GDPR:

Right to be Informed:

- Right to know what personal data is being collected and how it will be used
- ELI Schools provides privacy notices

Right of Access (Subject Access Request):

- Right to obtain copy of personal data ELI Schools holds about them
- Must respond within 1 month, free of charge (unless request excessive)

Right to Rectification:

- Right to have inaccurate or incomplete personal data corrected
- Must respond within 1 month

Right to Erasure ("Right to be Forgotten"):

- Right to have personal data erased in certain circumstances (data no longer necessary, consent withdrawn, unlawfully processed, legal obligation to erase)
- Not absolute right (e.g., cannot erase if retention required by law or legitimate interest)

Right to Restrict Processing:

- Right to request restriction of processing in certain circumstances (accuracy disputed, unlawful processing, no longer needed but individual wants retained for legal claims)

Right to Data Portability:

- Right to receive personal data in structured, commonly used, machine-readable format and transmit to another controller
- Applies when processing based on consent or contract and carried out by automated means
- Limited applicability to ELI Schools

Right to Object:

- Right to object to processing based on legitimate interests or for direct marketing
- ELI Schools must stop processing unless compelling legitimate grounds

Rights Related to Automated Decision-Making and Profiling:

- Right not to be subject to decisions based solely on automated processing

9.1 Data Protection Policy – Organisation

QA Area(s)	• Information and Data Management • Governance and Management of Quality		
Applies to	☑ Staff only	☐ Learners only	☐ Staff and learners
Policy Owner	Managing Director		

Purpose

The purpose of this policy is to establish ELI Schools' organizational commitment and approach to data protection compliance, ensuring that all processing of personal data complies with the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

Scope

This policy applies to:

- ELI Schools as an organization (data controller)
- All processing of personal data by ELI Schools
- All locations
- All personal data (students, staff, applicants, agents, host families, others)

Policy Statement

Commitment to Data Protection:

ELI Schools is committed to protecting the privacy and personal data of all individuals whose data we process. We will:

- Comply fully with GDPR and Data Protection Act 2018
- Process personal data lawfully, fairly, and transparently
- Collect and use only necessary personal data
- Keep personal data secure
- Respect data subject rights
- Be accountable and demonstrate compliance

DATA CONTROLLER

ELI Schools is the data controller for personal data processed in connection with our education and training provision and related activities.

Data Controller Details:

- **Organization:** LT Education Abroad Limited, trading as ELI Schools
- **Address:** 7 Herbert Place, Dublin 2, D02EH93
- **Data Protection Contact:** Peter Hutchinson, peter@elischools.com

Types Of Personal Data Processed

ELI Schools processes personal data relating to:

Students:

- Contact and biographical details
- Academic records
- Financial records
- Accommodation data
- Support and welfare data (including special category data where disclosed: disabilities, medical conditions, safeguarding concerns)
- Immigration data
- Communications
- Images (photographs, videos)

Staff:

- Contact and biographical details
- Employment records
- Qualifications and Garda vetting
- Performance and CPD records
- Payroll data
- Communications
- (Special category data where disclosed: medical conditions, disciplinary records)

Applicants (prospective students and staff):

- Application data
- Communications

Other Data Subjects:

- Agents, partners, host families, parents/guardians, suppliers, visitors: Contact details, communications, contractual data as necessary

Purposes Of Processing

ELI Schools processes personal data for the following purposes:

Providing Education and Training:

- Enrolling students
- Delivering programmes
- Assessing and recording student achievement
- Issuing certificates
- Providing academic and pastoral support
- Managing attendance and progression

Student Administration:

- Communicating with students
- Arranging accommodation
- Organizing activities and social programmes
- Processing fees and financial administration

Compliance with Legal Obligations:

- Immigration reporting (INIS/GNIB)
- Tax compliance
- Health and safety compliance
- Safeguarding obligations (Children First Act)
- Quality assurance (QQI)

Quality Assurance and Improvement:

- Gathering feedback
- Monitoring and evaluating provision
- Accreditation and inspection
- Research and analysis (anonymized where possible)

Employment and HR:

- Recruiting staff
- Administering employment
- Payroll and benefits
- Performance management and development
- Compliance with employment law

Marketing and Communications:

- Promoting ELI Schools
- Communicating with prospective students, agents, partners
- (Only with consent where required)

Security and Safety:

- Premises security (CCTV where used)
- Safeguarding children and adults at risk
- Health and safety
- Incident management

Legal Claims and Disputes:

- Establishing, exercising, or defending legal claims
- Complaints and appeals

Legal Bases for Processing

ELI Schools processes personal data under the following legal bases:

For Students:

- **Contract:** Processing necessary for education contract (enrolment, teaching, assessment, support, issuing certificates)
- **Legal Obligation:** Compliance with immigration law, tax law, safeguarding law, quality assurance requirements
- **Legitimate Interests:** Quality assurance, security, legal claims (where not covered by contract or legal obligation)
- **Consent:** Marketing (where consent obtained), photographs for promotional use, optional activities or data collection

For Staff:

- **Contract:** Employment contract performance
- **Legal Obligation:** Tax, PRSI, employment law compliance, Garda vetting (required for safeguarding)
- **Legitimate Interests:** Quality assurance, security
- **For Special Category Data:**
- **Explicit Consent:** Disabilities, medical conditions disclosed for reasonable accommodations or extenuating circumstances
- **Substantial Public Interest:** Safeguarding data (child protection legal obligation)
- **Employment:** Staff medical data for sick leave, occupational health

Data Protection Principles

ELI Schools processes all personal data in accordance with GDPR principles:

Lawfulness, Fairness, Transparency:

- Legal basis for all processing
- Fair processing
- Transparent: Privacy notices provided; individuals informed

Purpose Limitation:

- Data collected for specified purposes
- Not used for incompatible purposes

Data Minimization:

- Only necessary data collected and processed

Accuracy:

- Data kept accurate and up to date
- Mechanisms for individuals to update or correct data

Storage Limitation:

- Data retained only as long as necessary
- Retention periods defined
- Secure disposal when no longer needed

Integrity and Confidentiality:

- Appropriate security measures (technical and organizational)
- Protection against unauthorized access, loss, damage

Accountability:

- ELI Schools demonstrates compliance
- Documentation, policies, training, audits

Data Subject Rights

ELI Schools respects and facilitates data subject rights:

- **Right to be Informed:** Privacy notices provided
- **Right of Access:** Subject access requests handled (see Policy 10.3)
- **Right to Rectification:** Inaccurate data corrected
- **Right to Erasure:** Data erased where required (subject to legal retention obligations)
- **Right to Restrict Processing:** Restriction applied where appropriate
- **Right to Data Portability:** Provided where applicable
- **Right to Object:** Objections considered; processing stopped unless compelling legitimate grounds
- **Rights re Automated Decision-Making:** Not applicable (no automated decision-making at ELI Schools)

Data Security

ELI Schools implements appropriate security measures:

Technical Measures:

- Encryption (sensitive data)
- Access controls (passwords, role-based access)
- Firewalls, antivirus protection
- Secure systems and backups
- Secure disposal (shredding, secure deletion)
- Incident response procedures
- Contracts with data processors
- Physical security (locked premises, restricted access)

Data Breaches

In event of data breach:

- Breach contained and assessed
- Data Protection Commission notified within 72 hours (if breach poses risk to individuals)
- Affected individuals notified (if high risk)

Data Retention and Disposal

Personal data retained only as long as necessary:

- **Student records:** 7 years after completion
- **Staff records:** 7 years after employment ends
- **Financial records:** 7 years (tax law requirement)
- **Safeguarding records:** Long-term retention per Children First guidance
- **Other records:** Specified retention periods (see Policy 10.3)

After retention period: Secure disposal (shredding, secure deletion).

THIRD PARTY PROCESSORS

When third parties process data on behalf of ELI Schools:

- Due diligence conducted
- Data Processing Agreements in place
- Processors provide sufficient guarantees of security and compliance
- Monitoring of compliance

INTERNATIONAL DATA TRANSFERS

Personal data transferred outside EEA only where:

- Recipient country has adequacy decision, OR
- Appropriate safeguards in place (Standard Contractual Clauses), OR
- Derogation applies (consent, contract, public interest)

ELI Schools minimizes international transfers; where necessary, ensures compliance.

PRIVACY NOTICES

ELI Schools provides clear privacy notices to all data subjects, informing them:

- Who we are (data controller)
- What personal data we collect
- Why we collect it (purposes)
- Legal basis for processing
- Who we share data with
- How long we keep data
- Data subject rights
- How to contact us and how to complain to Data Protection Commission

Version	1.0
Date Approved	March 2026
Approved by	Board of Directors
Next Review Date	March 2027

Related legislation, regulation or guidelines:

- General Data Protection Regulation (GDPR) (EU) 2016/679
- Data Protection Act 2018 (Ireland)
- Children First Act 2015 (safeguarding data)
- Core Statutory Quality Assurance Guidelines 2016 (QQI)
- Code of Practice for Provision of Programmes of English Language Education to International Learners

9.2 Data Protection Policy – Employees

QA Area(s)	• Information and Data Management		
Applies to	☑ Staff only	☐ Learners only	☐ Staff and learners
Policy Owner	Managing Director		

Purpose

The purpose of this policy is to establish the responsibilities and obligations of all ELI Schools employees (staff) in relation to data protection, ensuring that all staff understand their role in protecting personal data and complying with GDPR.

Scope

This policy applies to:

- All staff at ELI Schools (full-time, part-time, freelance, temporary, volunteers, at all locations)
- All personal data handled by staff in the course of their employment
- All data processing activities undertaken by staff

Policy Statement

Staff Responsibilities for Data Protection:

All ELI Schools staff have a responsibility to protect personal data and comply with data protection law. Staff must:

- Understand and comply with GDPR and ELI Schools' data protection policies
- Handle personal data responsibly, securely, and confidentially
- Complete data protection training
- Report data breaches or security concerns immediately
- Respect individuals' privacy and data subject rights

Non-compliance with this policy may result in disciplinary action, up to and including dismissal. Serious breaches of data protection law may also result in personal liability and prosecution.

GENERAL PRINCIPLES FOR STAFF

When handling personal data, staff must:

Only Access Data You Need:

- Access only personal data necessary for your role
- "Need to know" principle
- Do not access data out of curiosity or for unauthorized purposes
- Unauthorized access is breach of data protection

Example:

- Teachers can access data about their own students (contact details, academic progress, attendance) - necessary for teaching role
- Teachers should NOT access data about students in other classes unless there's legitimate reason
- Office staff can access enrolment and financial data
- Office staff should NOT access confidential pastoral support or safeguarding data unless specifically authorized

Keep Data Confidential:

- Personal data is confidential
- Do not discuss or disclose personal data to unauthorized persons
- Conversations about students, staff, or others should be private, not in public
- Do not share personal data with family, friends, or social contacts
- Do not gossip or discuss individuals' personal matters

Example:

- Do not discuss student's disability, personal circumstances, or academic performance with colleagues who don't need to know
- Do not discuss student matters in café, on public transport, or in social settings where others could overhear
- Do not share information about students or staff on social media

Use Data Only for Authorized Purposes:

- Personal data collected for specific purposes (education, employment, administration)
- Use data only for those purposes, not for other purposes
- Do not use student or staff contact details for personal purposes

Example:

- Student email addresses may be used to send course information, not to send personal messages unrelated to course
- Staff should not use student data for personal social networking, dating, business purposes

Keep Data Accurate:

- If you notice inaccurate personal data, correct it or report it so it can be corrected
- Accuracy important for effective administration and fairness to individuals

Keep Data Secure:

- Protect personal data from unauthorized access, loss, damage
- Follow security procedures (see below)

Respect Data Subject Rights:

- Individuals have rights over their personal data
- Facilitate data subject rights requests (forward to Managing Director or Data Protection Lead)
- Respond to individuals' questions about their data

Report Concerns:

- If you suspect data breach, security weakness, or data protection violation, report immediately
- If you're unsure whether something is compliant, ask
- Better to ask than to risk breach

Specific Data Protection Obligations for Staff

Passwords and Authentication:

Requirements:

- Use strong passwords (at least 8 characters, mix of upper/lowercase, numbers, symbols)
- Do not share passwords with anyone (including colleagues, IT support - legitimate IT support will never ask for your password)
- Do not write passwords down in accessible places
- Change passwords regularly (every 3-6 months or when prompted)
- Use different passwords for different systems (don't reuse passwords)
- Use multi-factor authentication (MFA) where available
- Do not save passwords in browsers on shared computers
- **Rationale:** Passwords are first line of defense against unauthorized access.

Clear Desk and Clear Screen:

Requirements:

Clear Desk:

- Do not leave documents containing personal data on desk when away
- Lock documents in drawer or cabinet when not in use
- Do not leave sensitive documents visible to students, visitors, or other unauthorized persons
- At end of day, secure all documents

Clear Screen:

- Lock computer screen when leaving desk (even briefly)
- Log out of systems when finished
- Position screen so not visible to unauthorized persons (students, visitors)

Rationale: Prevents unauthorized viewing or taking of personal data; simple but effective measure

Email and Electronic Communications:

Requirements:

Sending Emails Containing Personal Data:

- Check recipient address carefully before sending (especially when using auto-complete)
- Use BCC (blind carbon copy) when sending to multiple recipients who don't know each other (so email addresses not disclosed to all recipients)
- Do not email sensitive personal data (medical data, safeguarding concerns, disciplinary matters) unless encrypted or using secure system
- Be cautious with "Reply All" - ensure all recipients should receive information
- Do not forward emails containing personal data to unauthorized persons

Receiving and Storing Emails:

- Do not leave email open and unattended on screen
- Delete emails containing personal data when no longer needed (within retention period)
- Spam and phishing: Do not click links or open attachments from unknown or suspicious senders; report suspicious emails to IT/management

Personal Email Accounts:

- Do not use personal email accounts (Gmail, Hotmail, etc.) for work-related communications containing personal data
- Use only ELI Schools email account for work
- Rationale: ELI Schools cannot control security or retention of personal email accounts

Use Of Devices (Computers, Laptops, Tablets, Phones):

ELI Schools Devices:

- Use only for work purposes (reasonable personal use may be acceptable but no processing personal data for personal purposes)
- Keep devices secure (password-protected, not left unattended)
- Do not install unauthorized software
- Report loss or theft immediately

Personal Devices:
Generally, personal devices (personal laptops, phones, tablets) should NOT be used for processing ELI Schools personal data

- If personal device use authorized by management (e.g., teacher using own laptop for lesson planning): Device must be password-protected, antivirus installed, data encrypted if storing personal data, device kept secure
- Do not store ELI Schools personal data on personal devices unless absolutely necessary and authorized
- If ELI Schools data on personal device, delete securely when no longer needed or when leave employment

USB Drives and Portable Storage:

- Minimize use (cloud storage or network drives preferred)
- If must use USB drive: Password-protected or encrypted, kept secure, data deleted after use
- Do not leave USB drives in computers or lying around
- Report loss immediately
- **Rationale:** Lost or stolen devices are common cause of data breaches; security measures mitigate risk.

Printing And Photocopying:

Requirements:

- Only print personal data when necessary (digital preferred)
- Collect printouts immediately from printer (do not leave sitting in printer tray where others could see)
- Do not print more copies than needed
- Shred or securely dispose of unwanted copies
- Be aware of who is around when printing/photocopying sensitive data
- **Rationale:** Printed documents easily lost, misplaced, or seen by unauthorized persons.

Disposing Of Personal Data:

Requirements:
Paper Documents:

- Shred documents containing personal data (cross-cut shredder)
- Do not just throw in regular bin
- Confidential waste bins provided for shredding

Digital Data:

- Delete when no longer needed (within retention period)
- Empty Recycle Bin / Trash (deletion not complete until emptied)
- For sensitive data, use secure deletion tools if available

Devices:

- When disposing of old devices (computers, phones, etc.), ensure data securely wiped or device destroyed
- IT support or management handles device disposal
- **Rationale:** Insecure disposal can result in data breaches; data can be recovered from bins or improperly disposed devices.

Working Remotely or in public:

Requirements:

- If working remotely (home, café, etc.), take extra care with security
- Use secure Wi-Fi (not public/open Wi-Fi for accessing personal data
- Privacy screens if working on laptop/tablet in public
- Do not discuss personal data on phone in public
- Secure documents and devices when working remotely

Rationale: Public and remote environments have higher risk of unauthorized viewing or access

Sharing Personal Data:

Requirements:

With Colleagues:

- Share only with colleagues who need to know for work purposes
- Use secure methods (internal email, secure shared drive)

With External Parties (Third Parties, Other Organizations):

- Share only when necessary and authorized
- Check: Is there legal basis? Is there data sharing agreement if required? Is sharing necessary and proportionate?
- Use secure methods (encrypted email, secure file transfer)
- Examples: Sharing safeguarding concerns with Tusla (statutory obligation)

Do NOT Share:

- With unauthorized persons
- With family, friends, social contacts
- On social media
- For unauthorized purposes

If Unsure Whether to Share: Ask manager or Data Protection Lead.

Consent And Permissions:

When collecting personal data from individuals:

- Explain what data you're collecting and why (transparency)
- If processing based on consent, obtain clear, informed consent
- Provide privacy notice or direct individual to privacy notice

Example:

- When enrolling student, explain how their data will be used; provide Student Privacy Notice
- If taking photographs for promotional use, obtain consent

Do not:

- Assume consent or that "it's obvious"
- Pre-tick consent boxes
- Make consent a condition for service unless genuinely necessary

Children And Vulnerable Adults:

Extra care when handling personal data of children (under-18s) and vulnerable adults:

- Higher duty of care
- Strict confidentiality (safeguarding data especially sensitive)
- Only share safeguarding concerns with authorized persons (Designated Liaison Person, management, Tusla/Gardaí as appropriate)
- Parental involvement (parents informed of data processing; for younger children, parental consent may be required)

If handling safeguarding data:

- Strictest confidentiality
- Secure storage
- "Need to know" very limited
- Follow safeguarding procedures (Section 15)

Photographs And Videos:

Personal data includes images (photographs, videos) of identifiable individuals.

When taking or using photographs/videos of students or staff:

- Obtain consent (especially for promotional use)
- Explain how images will be used
- Respect refusals (if someone doesn't want to be photographed)
- Store images securely
- Do not share on personal social media without consent
- Delete when no longer needed

Students photographing/filming:

- Students should not photograph or film other students or staff without consent
- Teachers should remind students of this (privacy and respect)

Social media:

Staff use of social media:

Personal Social Media:

- Staff entitled to personal social media use
- However: Do not post about students, colleagues, or work matters involving personal data
- Do not "friend" or connect with current students on personal social media (professional boundary)
- Do not post photographs of students without consent
- Be aware that public posts may reflect on ELI Schools (professional conduct expected)

ELI Schools Official Social Media:

- If authorized to manage ELI Schools social media, follow data protection rules
- Obtain consent before posting identifiable images of students
- Do not post personal data unnecessarily
- **Rationale:** Social media is public and permanent; data breaches or unprofessional conduct on social media can have serious consequences.

Work Email, Teams or Mobile Phones

Staff use of ELI provided technology, phones, email etc:

- Do not use ELI provided technology or chat to discuss personal behaviour, character or appearance of students, colleagues or service providers
- Always consider that comments made on ELI provided technology can be requested at any time and must be shared with individuals concerned.
- Employees may be held liable for comments made about students, colleagues or service providers if deemed defamatory or derogatory.

Data Subject Requests:

If student, staff member, or other individual makes data subject request (access, rectification, erasure, etc.):

Do:

- Forward request to Managing Director or Data Protection Lead immediately
- Do not ignore or delay
- Be helpful and polite

Do NOT:

- Attempt to handle request yourself (unless specifically authorized)
- Ignore request
- Delete or alter data in response to request without authorization (this could be destruction of evidence

Data Breaches:

Data breach: Unauthorized access, loss, disclosure, alteration, or destruction of personal data.

Examples:

- Lost laptop or USB drive containing personal data
- Email sent to wrong recipient with personal data
- Unauthorized person accessing data
- Documents left on train
- Hacking or cyber attack

Immediately:

- **Contain:** If possible, contain breach (e.g., if sent email to wrong recipient, contact recipient and ask them to delete)
- **Report:** Report to your manager and Managing Director or Data Protection Lead immediately (same day, or as soon as you become aware)
- **Document:** Write down what happened (facts)

Do NOT:

- Hide breach or hope it goes unnoticed
- Delay reporting
- Try to fix it yourself without reporting (even if you think you've fixed it)

Why Immediate Reporting Critical:

- Legal obligation to notify Data Protection Commission within 72 hours of becoming aware
- Early reporting allows timely response, mitigation, notification
- Delayed reporting can result in greater harm and penalties

No Blame (for Honest Mistakes):

- ELI Schools recognizes that honest mistakes can happen
- Staff will not be punished for reporting genuine accidental breaches (e.g., accidentally sending email to wrong recipient)

However, repeated carelessness, reckless behaviour, or deliberate breaches are disciplinary matters

Covering up breach is far more serious than accidental breach itself.

Training:

All staff must:

- Complete data protection training
- Complete refresher training annually
- Training is mandatory (not optional)
- Training covers: GDPR principles, ELI Schools policies, security, confidentiality, handling data, data breaches

Training Records:

- Completion of training recorded
- Managers monitor compliance

Questions And Concerns:

If you have questions, concerns, or are unsure about data protection:

Ask:

- Your manager
- Managing Director
- Data Protection Lead
- Quality Officer
- **Better to ask than to guess and risk breach.**

Reporting Concerns:

- If you believe data protection is being violated (by colleague, manager, organization), report concern to Managing Director or Data Protection Lead
- Concerns will be taken seriously and investigated
- Whistleblowing protections apply (staff protected from retaliation for raising genuine data protection concerns)

Consequences of Non-Compliance

Data protection compliance is serious obligation.

Non-compliance can result in:

For ELI Schools:

- Legal liability
- Fines from Data Protection Commission (up to €20 million or 4% of annual turnover, whichever higher)
- Legal claims from affected individuals
- Reputational damage
- Loss of trust (students, staff, partners)
- Loss of accreditation or registration

For Individual Staff Member:

- Disciplinary action (warning, suspension, dismissal)
- Personal liability in some cases (particularly if criminal breach - unlawfully obtaining or disclosing personal data)
- Prosecution in serious cases
- Damage to professional reputation

Levels of Disciplinary Action

Minor Breach (unintentional, first time, no harm):

- Example: Accidentally sent email to wrong recipient; reported immediately; no sensitive data
- Response: Verbal warning, retraining, reminder of policies

Moderate Breach (carelessness, repeated minor breaches, potential harm):

- Example: Repeatedly leaving documents on desk; repeatedly failing to lock screen; moderate security lapse
- Response: Written warning, formal retraining, closer monitoring

Serious Breach (reckless, deliberate, causing harm, gross negligence):

- Examples: Deliberately accessing data without authorization; sharing confidential data inappropriately; losing device containing sensitive data due to gross negligence; covering up breach
- Response: Suspension, dismissal, possible reporting to authorities

Gross Misconduct (deliberate, malicious, criminal):

- Examples: Stealing personal data; selling data; deliberately destroying data; using data for fraud or harassment

Staff Responsibilities Summary

As ELI Schools staff member, you MUST:

✓ Complete data protection training
✓ Handle personal data responsibly and securely
✓ Keep data confidential
✓ Access only data you need for your role
✓ Use strong passwords and lock screens
✓ Be careful with emails and data sharing
✓ Keep devices and documents secure
✓ Dispose of data securely (shred documents)
✓ Report data breaches immediately
✓ Ask if unsure

You MUST NOT:

✗ Share personal data with unauthorized persons
✗ Discuss personal data publicly or on social media
✗ Use personal data for unauthorized purposes
✗ Access data out of curiosity
✗ Leave data or devices unsecured
✗ Ignore data breaches or security concerns
✗ Share passwords
✗ Use personal devices for work data without authorization
✗ Connect with students on personal social media

All staff required to read and acknowledge this policy:

- Policy provided during induction
- Staff sign acknowledgment form confirming they have read, understood, and will comply with policy
- Acknowledgment kept in personnel file

Staff Acknowledgment Form:

DATA PROTECTION POLICY - EMPLOYEE ACKNOWLEDGMENT
I, ________________________________ (name), acknowledge that:
I have received, read, and understood ELI Schools' Data Protection Policy - Employees (Policy 10.2)
I understand my responsibilities and obligations for protecting personal data and complying with GDPR
I understand the security requirements (passwords, clear desk/screen, email security, device security, etc.)
I understand the requirement to report data breaches immediately
I understand that non-compliance may result in disciplinary action
I commit to complying with this policy and all ELI Schools data protection policies
I will complete required data protection training
I will ask questions if unsure about data protection
Signature: ________________________________
Date: ________________________________

Version	1.0
Date Approved	March 2026
Approved by	Managing Director, Board of Directors
Next Review Date	March 2027

Related legislation, regulation or guidelines:

- General Data Protection Regulation (GDPR) (EU) 2016/679

9.3 Data Protection Governance Framework

QA Area(s)	• Information and Data Management • Governance and Management of Quality		
Applies to	☐ Staff only	☐ Learners only	☐ Staff and learners
Policy Owner	Managing Director		

Purpose

The purpose of this document is to provide a comprehensive, detailed framework for data protection governance, systems, and procedures at ELI Schools, ensuring systematic implementation of data protection compliance.

Scope

This framework covers:

- Data protection governance structure and responsibilities
- Records of processing activities
- Privacy notices
- Data subject rights procedures
- Data security procedures
- Data breach procedures
- Data retention and disposal
- Data Processing Agreements with third parties
- Training
- Monitoring and audit

PART A: DATA PROTECTION GOVERNANCE STRUCTURE

1. Roles and Responsibilities

Board of Directors:

- Ultimate accountability for data protection compliance
- Oversight of data protection governance
- Ensuring resources for compliance
- Receiving reports on data protection compliance, breaches, issues
- Ensuring data protection risks managed

Managing Director:

- Overall operational accountability for data protection
- Acts as Data Protection Officer or designates Data Protection Lead
- Ensuring policies and procedures implemented
- Approving data protection policies
- Responding to serious breaches or enforcement actions
- Liaison with Data Protection Commission if required
- Ensuring staff training
- Resources for compliance

Data Protection Officer / Data Protection Lead:

- Advising ELI Schools and staff on data protection obligations
- Monitoring compliance with GDPR and data protection policies
- Providing data protection training and awareness
- Conducting or coordinating Data Protection Impact Assessments
- Maintaining records of processing activities
- Handling data subject rights requests
- Investigating data breaches
- Liaison with Data Protection Commission
- Point of contact for data protection queries

PART B: RECORDS OF PROCESSING ACTIVITIES

GDPR Article 30 requires organizations to maintain records of processing activities.

3. Register of Data Processing Activities

ELI Schools maintains register documenting all data processing activities.

Register includes for each processing activity:

- Name and contact details of controller (ELI Schools)
- Purposes of processing
- Categories of data subjects (students, staff, etc.)
- Categories of personal data (contact details, academic records, etc.)
- Categories of recipients (who data is shared with - internal staff, external parties)
- Transfers to third countries (if any)
- Retention periods
- Description of technical and organizational security measures
- **Register format:** Spreadsheet or document; kept up to date; available for review by Data Protection Commission if requested.
- **Responsibility:** Data Protection Lead maintains register; reviewed annually.

Example Entries in Register:

Processing Activity 1: Student Enrolment and Administration

- **Controller:** ELI Schools
- **Purposes:** Enrolling students, delivering education, assessment, issuing certificates, administration
- **Legal Basis:** Contract (education contract with student)
- **Data Subjects:** Students (current, past, applicants)

Categories of Personal Data: Name, contact details, date of birth, nationality, passport number, photograph, academic records (level, programme, attendance, assessment results, certificates), financial records (fees, payments), accommodation data (if applicable), communications

- **Special Category Data:** Disabilities, medical conditions (if disclosed for reasonable accommodations or extenuating circumstances) - Legal basis: Explicit consent
- **Recipients (Internal):** Office staff, Programme Leaders, teachers, Senior Academic Manager, Student Services Officer (on need-to-know basis)
- **Recipients (External):** Awarding bodies (if accredited programmes - Cambridge, Trinity, etc.), university partners (for pathway students - transcripts), immigration authorities (INIS/GNIB - visa letters, attendance reporting if required), parents/guardians (for under-18s)
- **Transfers to Third Countries:** Transcripts sent to universities outside EEA (legal basis: performance of contract between student and university); data shared with agents outside EEA (legal basis: consent or performance of contract)
- **Retention Period:** 7 years after student completes programme
- **Security Measures:** Access controls (role-based access), password protection, encryption of sensitive data, secure servers, backups, physical security (locked premises), staff training, confidentiality

Processing Activity 2: Staff Employment and HR

- **Controller:** ELI Schools
- **Purposes:** Recruiting, employing, managing, paying staff; performance management; compliance with employment law
- **Legal Basis:** Contract (employment contract), Legal obligation (tax, PRSI, Garda vetting)

- **Data Subjects:** Staff (current, past, applicants)
- **Categories of Personal Data:** Name, contact details, employment history, qualifications, Garda vetting, performance records (teaching observations, appraisals), CPD records, payroll data (salary, bank details, tax number, PRSI), communications
- **Special Category Data:** Medical data (if disclosed for sick leave, occupational health) - Legal basis: Employment; Disciplinary data (if applicable)
- **Recipients (Internal):** HR Manager, Managing Director, line managers (on need-to-know basis), payroll staff
- **Recipients (External):** Revenue (tax compliance), payroll service provider (if external - Data Processing Agreement), pension providers, references to prospective employers (with consent)
- **Transfers to Third Countries:** None typically
- **Retention Period:** 7 years after employment ends
- **Security Measures:** As above

Processing Activity 3: Quality Assurance and Evaluation

- **Controller:** ELI Schools
- **Purposes:** Monitoring and improving quality; compliance with QQI requirements; evaluation and research
- **Legal Basis:** Legitimate interests (maintaining educational quality and compliance)
- **Data Subjects:** Students (feedback, outcomes data), staff (feedback, observations)
- **Categories of Personal Data:** Aggregated outcomes data (pass rates, attendance rates - usually anonymized); student feedback (anonymous surveys but may contain identifiable comments); staff feedback (anonymous); teaching observation reports (staff performance data)
- **Special Category Data:** None typically (QA data usually anonymized)
- **Recipients (Internal):** Quality Officer, Senior Academic Manager, Programme Leaders, Academic Committee, Board (aggregated data)
- **Recipients (External):** QQI (inspection reports, data); external examiners (samples of student work - may contain personal data)
- **Transfers to Third Countries:** None
- **Retention Period:** 7 years
- **Security Measures:** As above; anonymization where possible
- **Processing Activity 4: Safeguarding (for Under-18 Programmes)**
- **Controller:** ELI Schools
- **Purposes:** Child protection; ensuring safety and welfare of children; compliance with Children First Act
- **Legal Basis:** Legal obligation (Children First Act), Substantial public interest (child protection)
- **Data Subjects:** Children (students under 18), parents/guardians, staff, others involved in concerns
- **Categories of Personal Data:** Safeguarding concerns, reports, assessments, communications, child's details, parent details
- **Special Category Data:** Data about child's welfare, health, safety (inherently special category) - Legal basis: Substantial public interest
- **Recipients (Internal):** Designated Liaison Person (Student Services Officer), Managing Director, relevant staff on strict need-to-know
- **Recipients (External):** Tusla (Child and Family Agency) - mandatory reporting, Gardaí (if criminal concern), legal advisors (if needed)
- **Transfers to Third Countries:** None
- **Retention Period:** Indefinitely or very long term (per Children First guidance - safeguarding information may be relevant many years later)
- **Security Measures:** Strictest security and confidentiality; separate secure storage; access highly restricted; encrypted; secure communication with Tusla/Gardaí

Processing Activity 5: Marketing and Communications

- **Controller:** ELI Schools
- **Purposes:** Promoting ELI Schools; communicating with prospective students and agents
- **Legal Basis:** Consent (for electronic marketing communications), Legitimate interests (for general marketing and business communications)
- **Data Subjects:** Prospective students, education agents, subscribers to newsletters, website visitors
- **Categories of Personal Data:** Name, contact details (email, phone), nationality, programme interests, communications
- **Special Category Data:** None
- **Recipients (Internal):** Marketing staff, office staff
- **Recipients (External):** Email marketing platform (e.g., Mailchimp - Data Processing Agreement), website hosting provider (Data Processing Agreement)
- **Transfers to Third Countries:** Email marketing platform may have servers in US (Standard Contractual Clauses or adequacy - check)
- **Retention Period:** Until consent withdrawn or 3 years of inactivity (then delete)
- **Security Measures:** As above; unsubscribe mechanism for marketing emails

Register reviewed and updated annually or when significant new processing activity added.

PART C: PRIVACY NOTICES

GDPR Article 13 and 14 require providing privacy information to data subjects.

4. Privacy Notices Provided

ELI Schools provides privacy notices to all data subjects:

A. Student Privacy Notice:

- Provided at application/enrolment
- Available on website
- Explains: What student data we collect, why, legal basis, how we use it, who we share it with, retention, rights, how to contact us

B. Staff Privacy Notice:

- Provided at recruitment
- Explains: What staff data we collect, why, legal basis, how we use it, who we share it with, retention, rights, how to contact us

C. Website Privacy Policy:

- Published on website
- Covers: Website visitors, cookies, contact forms, email subscribers

D. Junior Programme Parent/Guardian Privacy Notice:

- Provided to parents/guardians of under-18 students
- Explains: What data we collect about child, why, safeguarding, communication with parents, rights

E. Other Privacy Notices (as needed):

- Host families, agents, applicants, etc. - as appropriate

5. Privacy Notice Content

Privacy notices include (as per GDPR Article 13):

See ELI Schools Data Privacy Notice

PART D: DATA SUBJECT RIGHTS PROCEDURES

Individuals can exercise their rights under GDPR. ELI Schools has procedures for handling requests.

6. Handling Data Subject Rights Requests

Types of Requests:

- Subject Access Request (Right of Access) - Copy of personal data
- Rectification - Correct inaccurate data
- Erasure ("Right to be Forgotten") - Delete data
- Restriction - Restrict processing
- Data Portability - Receive data in structured format
- Objection - Object to processing
- Procedure for Subject Access Requests (SAR) - Most Common**:**

Step 1: Request Received

How Request May Be Received:

- Email
- Letter
- In person
- Verbally (though written preferred)

Who May Receive:

- Any staff member may receive request
- If staff member receives request, forward immediately to Data Protection Lead

Request Must:

- Be from data subject (or authorized representative with proof of authority)
- Clearly indicate individual wants to access their personal data
- May need to verify identity (especially if request by email - may ask for photo ID to prevent disclosing data to wrong person)

Step 2: Acknowledge and Verify

Data Protection Lead:

- Acknowledges request within 2 working days
- Verifies identity if needed (request copy of photo ID, or ask questions to confirm identity)
- If request from representative (e.g., parent, solicitor), verify authority (authorization letter, power of attorney, etc.)

Step 3: Gather Data

Data Protection Lead coordinates:

Identify what personal data ELI Schools holds about individual (check all systems and records: student management system, email, paper files, quality assurance data, safeguarding records if applicable, etc.)

Gather all data

Review data for:

- Third party data (data about other people) - must redact to protect others' privacy
- Legal professional privilege (if data contains privileged legal advice) - can withhold
- Manifestly unfounded or excessive requests - can refuse or charge fee (rare)

Step 4: Prepare Response

Data Protection Lead prepares:

- Copy of all personal data (usually PDF or Word document)
- Organized clearly (not just raw data dump but understandable)
- Cover letter explaining:
- Data provided
- Sources of data
- Purposes of processing
- Recipients
- Retention period
- Rights (rectification, erasure, complaint, etc.)

If any data is withheld (third party data redacted, legal privilege), explain why.

Step 5: Provide Data

- **Timeline:** Within 1 month of receiving request (can extend by 2 months if complex, but must inform individual within 1 month)
- **Method:** Secure method (encrypted email, registered post, hand delivery)
- **No Fee:** Free of charge (unless request manifestly unfounded or excessive - can refuse or charge reasonable fee)

Step 6: Document

- Record request and response
- Keep in data subject requests log
- Accountability

Procedure for Other Rights Requests:

Rectification:

- If individual points out inaccurate data, correct it promptly (within 1 month)
- Notify individual when corrected
- If data has been shared with third parties, inform them of correction where feasible

Erasure:

- Assess whether legal basis for erasure exists (data no longer necessary, consent withdrawn, unlawful processing, legal obligation to erase)
- If legal basis exists and no overriding reason to retain (e.g., legal obligation to retain for 7 years), erase data
- If cannot erase (legal retention requirement), explain why
- Within 1 month

Restriction:

- If individual requests restriction (e.g., disputing accuracy, while accuracy is verified), restrict processing (do not process data except for storage, or with consent, or for legal claims)
- Within 1 month

Data Portability:

- If applicable (processing based on consent or contract, carried out by automated means), provide data in structured, machine-readable format (e.g., CSV, JSON)
- Within 1 month

Objection:

- If individual objects to processing based on legitimate interests, assess: Are there compelling legitimate grounds that override individual's interests?
- If not, stop processing
- If objection to marketing, always stop (absolute right)
- Within 1 month

7. Data Subject Requests Log

Data Protection Lead maintains log of all data subject requests:

Date Received	Type of Request	Data Subject	Status	Date Completed	Outcome	Notes
15/03/2024	Subject Access Request	John Smith (former student)	Completed	10/04/2024	Data provided	Verified identity; provided student records
22/04/2024	Rectification	Jane Doe (current student)	Completed	25/04/2024	Data corrected	Corrected email address in records
05/05/2024	Erasure	Mark Jones (former student)	Completed	08/05/2024	Refused	Retention period not expired; legal obligation to retain 7 years

Log reviewed periodically; trends analysed; process improvements identified.

PART E: DATA SECURITY PROCEDURES

ELI Schools implements technical and organizational security measures.

8. Technical Security Measures

A. Access Controls:

- **User accounts:** Each staff member has individual user account (no shared accounts)
- **Passwords:** Strong password policy (minimum 8 characters, complexity, expiry every 6 months)
- **Role-based access:** Staff can only access data necessary for their role (not all staff access all data)
- **Multi-factor authentication (MFA):** Used where available (especially for administrative accounts)
- **Access reviews:** Periodic review of who has access to what; remove unnecessary access

B. Encryption:

- **Data at rest:** Sensitive data encrypted on servers and devices (full disk encryption on laptops)
- **Data in transit:** Encrypted transmission (HTTPS for websites, TLS for email, secure file transfer for sensitive files)

C. Firewalls and Antivirus:

- Firewalls protect network
- Antivirus software on all devices (updated regularly)
- Malware protection

D. Secure Systems:

- Reputable, secure software and platforms (student management systems, email, cloud storage)
- Systems kept up to date (security patches applied promptly)
- Regular security updates

E. Backups:

- Regular backups of all data (daily or weekly depending on system)
- Backups stored securely (encrypted, offsite or cloud backup)
- Backup restoration tested periodically (ensure backups work)
- Backups retained for specified period (30 days to 1 year typically)

F. Secure Disposal:

- Digital data: Secure deletion (not just delete but overwrite; secure deletion tools; or physical destruction of storage media)
- Paper records: Cross-cut shredding or incineration
- Devices: Data wiped securely before disposal or reuse

9. Organizational Security Measures

A. Policies and Procedures:

- This framework and Policies 10.1, 10.2
- Clear policies on data protection and security
- Staff aware of policies

B. Staff Training:

- All staff trained in data protection (induction and annual refresher)
- Training covers: GDPR, policies, security, confidentiality, data breaches

- Training completion monitored

C. Confidentiality:

- All staff understand confidentiality obligations
- Contractual confidentiality clauses in employment contracts
- Culture of confidentiality

D. Access Controls (Organizational):

- "Need to know" principle
- Only authorized staff access data
- Physical access controls (locked offices, restricted access to sensitive areas)

E. Clear Desk and Screen Policy:

- Staff lock screens when away
- Staff secure documents when not in use
- No personal data left visible to unauthorized persons

F. Secure Communications:

- Caution with email (check recipients, use BCC for group emails, encrypt sensitive data)
- Secure methods for transferring sensitive data

G. Remote Working Security:

- If staff work remotely, security guidance provided (secure Wi-Fi, VPN if available, physical security of documents and devices)

H. Visitor Management:

- Visitors signed in and supervised
- Visitors not left in areas where they could access personal data

I. Contracts with Processors:

- Data Processing Agreements with all third parties processing data on behalf of ELI Schools
- Agreements specify security obligations

J. Incident Response:

- Data breach response procedure (see below)
- Staff know to report breaches immediately

K. Physical Security:

- Premises secured (locks, alarms, CCTV if used)
- Restricted access to offices and storage areas containing personal data
- Secure storage (locked cabinets for paper records, secure servers for digital data)

10. Password Policy

All staff must comply with password policy:

Requirements:

- **Minimum length:** 8 characters (12+ recommended)
- **Complexity:** Mix of uppercase, lowercase, numbers, symbols

- **Not dictionary words or easily guessable** (not "password", "123456", name, birthday)
- **Unique:** Different password for each system (not reusing passwords)
- **Expiry:** Change password every 6 months (or when prompted by system)
- **No sharing:** Never share passwords
- **Storage:** Use password manager if needed (not written on sticky notes); if must write down, store securely (locked drawer)

Enforcement:

- Systems enforce password complexity and expiry where possible
- IT support configures systems for password requirements

Compromise:

- If password compromised (disclosed, stolen, used by unauthorized person), change immediately and report to IT support/management

11. Backup and Business Continuity

Regular backups ensure data not lost due to technical failure, disaster, or cyber-attack.

Backup Policy:

What is Backed Up:

- Student management system data
- Financial data
- Email (if not cloud-based with provider's backup)
- Documents and files (server, shared drive)
- Website (if self-hosted)

Frequency:

- Critical systems: Daily backups
- Other systems: Weekly backups

Storage:

- Backups stored securely
- Offsite or cloud backup (so not lost if onsite disaster)
- Encrypted

Retention:

- Backups retained for specified period (typically 30 days to 1 year, depending on system and data criticality)
- Old backups securely deleted after retention period

Testing:

- Backup restoration tested periodically (at least annually)
- Ensures backups are working and data can be recovered

Business Continuity:

- Backup strategy part of business continuity plan
- In event of data loss (hardware failure, ransomware, disaster), data can be recovered from backups
- Recovery Time Objective (RTO): How quickly data must be recovered (e.g., within 24 hours for critical systems)

- Recovery Point Objective (RPO): How much data loss is acceptable (e.g., lose maximum 1 day of data if daily backups)

Responsibility:

- IT support (internal or external) manages backups
- Office Manager monitors backup status
- Managing Director ensures backup strategy adequate

Part F: Data Breach Procedures

- **Data breach:** Breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

12. Data Breach Response Procedure

Step 1: Detection and Reporting

Breach Detected By:

- Staff member discovers breach (e.g., realizes sent email to wrong person, lost laptop, unauthorized access detected)
- IT support detects breach (e.g., cyber-attack, system compromise)
- Individual reports breach to us (e.g., "I received email that wasn't meant for me")
- Third party notifies us (e.g., processor reports breach)

Immediate Reporting:

- **Anyone who detects or suspects breach must report immediately** (same day, or as soon as aware)
- **Report to:** Managing Director and Data Protection Lead
- **Methods:** Phone call (if urgent), email, in person
- **Out of hours emergency:** Emergency contact number for serious breaches

What to Report:

- What happened (facts)
- When it happened (date, time)
- What data affected (type of data, how much data, number of individuals)
- How breach occurred
- Any immediate action taken

Step 2: Containment

Immediate Actions to Contain Breach (if possible):

Examples:

- **Email to wrong recipient:** Contact recipient, ask to delete email, confirm deletion
- **Lost device:** Remote wipe device if capability exists
- **Unauthorized access:** Change passwords, disable compromised accounts, block access
- **Cyber-attack:** Isolate affected systems, disconnect from network to prevent spread
- **Responsibility:** Managing Director, IT support, relevant staff (whoever can take immediate action)
- **Priority:** Contain breach quickly to prevent further unauthorized access or loss

Step 3: Assessment

Data Protection Lead (with Managing Director) assesses breach:

Questions to Answer:

A. What data was breached?

- Type of data (contact details, financial, medical, safeguarding, etc.)
- Sensitivity (highly sensitive special category data, or less sensitive data?)
- Volume (how much data? how many individuals affected?)

B. What happened?

- Nature of breach (unauthorized access, loss, disclosure, alteration, destruction)
- Cause (human error, cyber-attack, theft, system failure, etc.)
- How did it happen (sequence of events)

C. Who is affected?

- Number of individuals
- Categories (students, staff, children, vulnerable adults, etc.)

D. What are the risks to individuals?

Potential consequences for individuals:

- Identity theft or fraud
- Financial loss
- Damage to reputation
- Psychological distress
- Physical harm (in extreme cases - e.g., safeguarding data breach)
- Discrimination
- **Severity:** High risk, moderate risk, low risk?
- **Likelihood:** Are consequences likely or unlikely?

E. What is the risk assessment?

- **No risk or low risk:** Minor breach, non-sensitive data, small number of people, no realistic harm
- **Risk:** Some potential for harm, but not severe
- **High risk:** Significant potential for serious harm (e.g., breach of sensitive data, large scale breach, children involved, etc.)

Step 4: Notification Obligations

Based on risk assessment:

A. Notification to Data Protection Commission (DPC):

- **Mandatory if:** Breach is likely to result in a risk to individuals' rights and freedoms (unless breach is unlikely to result in risk)
- **Timeline:** Within 72 hours of becoming aware of breach
- **How:** Online notification form on DPC website: www.dataprotection.ie

What to Include:

- Nature of breach
- Categories and approximate number of data subjects affected
- Categories and approximate number of records affected
- Contact point (Data Protection Lead)
- Likely consequences

- Measures taken or proposed to address breach and mitigate harm
- If notification delayed beyond 72 hours, reasons for delay

If information not all available within 72 hours: Submit initial notification with available information, then follow-up with additional information when available

Do NOT Delay Notification hoping to gather all information; better to notify promptly with what you know.

B. Notification to Individuals:

- **Mandatory if:** Breach is likely to result in a high risk to individuals' rights and freedoms
- **Timeline:** Without undue delay (as soon as reasonably possible after breach)
- **How:** Email, letter, or other direct communication (phone if urgent)

What to Include (in clear, plain language):

- Nature of breach (what happened)
- Contact point (Data Protection Lead, phone, email)
- Likely consequences
- Measures taken to address breach
- Measures individuals can take to protect themselves (e.g., change passwords, monitor accounts, report suspicious activity)
- Apology

Exception (Can Omit Individual Notification if High Risk BUT):

- Taken measures that render data unintelligible (e.g., breach of encrypted data and no one has decryption key), OR
- Taken subsequent measures ensuring high risk no longer likely, OR
- Notification would involve disproportionate effort (very large number of individuals) - then use public communication (website, press, etc.)

In practice, if notification to DPC required (risk to individuals), usually should notify individuals too (unless exception applies).

C. Notification to Other Parties:

May Need to Notify:

- **Gardaí (Police):** If criminal activity involved (theft, cyber attack, fraud)
- **Cyber Insurance Provider:** If ELI Schools has cyber insurance
- **Data Processors:** If breach at processor, processor must notify ELI Schools; if breach at ELI Schools affects processor's data, may need to notify
- **Professional Bodies, Regulators:** QQI, ACELS (if breach affects our compliance or operations)
- **Parents/Guardians:** If breach involves children, parents should be notified

Step 5: Investigation

Data Protection Lead (with assistance from IT support, relevant staff) investigates:

Questions:

- What exactly happened? (detailed timeline, root cause)
- Why did it happen? (vulnerability, human error, attack, etc.)
- Could it have been prevented? (were security measures adequate?)
- Were policies and procedures followed? (was staff member negligent or did they follow procedures?)
- What are the lessons learned?

- **Investigation documented:** Incident report with findings

Step 6: Remediation and Mitigation

Actions to Address Breach and Prevent Recurrence:

Immediate Remediation:

- Fix the vulnerability that caused breach (patch security hole, correct process, etc.)
- Recover lost data (from backups if applicable)
- Secure systems

Support for Affected Individuals:

- Provide advice and support (e.g., advise to change passwords, monitor accounts)
- Consider offering credit monitoring or identity theft protection if financial data breached (though this can be expensive)
- Apologize
- Be responsive to individuals' concerns

Prevent Recurrence:

- Identify root cause and address
- Implement additional security measures if needed
- Staff training or retraining (if human error)
- Update policies or procedures
- Disciplinary action if staff negligence or misconduct

Examples:

- Breach cause: Lost unencrypted laptop → Action: Ensure all laptops encrypted, policy requiring devices secured
- Breach cause: Email to wrong recipient → Action: Staff training on email security, implement "delayed send" feature
- Breach cause: Cyber-attack exploiting software vulnerability → Action: Update software, improve monitoring, staff training on phishing

Step 7: Documentation

Data Protection Lead documents breach in Data Breach Log:

Log Includes:

- Date and time of breach
- Date became aware
- Nature of breach
- Data affected
- Number of individuals affected
- Risk assessment
- Notification to DPC (yes/no, date)
- Notification to individuals (yes/no, date, method)
- Notifications to other parties
- Investigation findings (cause, root cause)
- Remediation actions taken
- Preventive measures implemented

- Lessons learned
- **Documentation Required by GDPR:** Even if breach not notified to DPC (because no risk), must still document breach internally (accountability).
- **Data Breach Log Retained:** Indefinitely (for accountability, audit, learning)

Step 8: Review and Learning

After breach resolved:

Review:

- What went well in response?
- What could have been done better?
- Are security measures adequate?
- Do policies need updating?
- Is further training needed?

Learning:

- Share lessons learned with staff (without blaming individuals)
- Update procedures based on learning
- Continuous improvement

Report to Governance:

- Serious breaches reported to Board of Directors
- All breaches summarized in periodic reports to Board and Academic Committee (anonymized, aggregated)
- Oversight and accountability

13. Data Breach Log

Data Protection Lead maintains Data Breach Log.

Example Entries:

Breach Date	Date Aware	Description	Data Affected	Individuals Affected	Risk	Notified DPC	Notified Individuals	Cause	Remediation	Preventive Measures
15/03/2024	15/03/2024	Email with student list sent to wrong recipient (another teacher)	Student names, email addresses (20 students)	20	Low (wrong recipient is staff member, deleted immediately, no harm)	No	No (low risk)	Human error (wrong recipient selected)	Email retrieved and deleted; sender reminded of care needed	Staff reminded of email security in team meeting

Part G: Data Retention and Disposal

14. Data Retention Schedule

Personal data retained only as long as necessary. Retention periods defined.

Retention Schedule:

Data Type	Retention Period	Rationale	Disposal Method
STUDENT DATA			
Student enrolment and contact records	7 years after completion	Transcript verification, queries, legal claims	Secure deletion (digital), shredding (paper)
Student academic records (attendance, assessment, certificates)	7 years after completion	Transcript verification, appeals, QA, legal claims	Secure deletion, shredding
Student financial records (fees, invoices, payments)	7 years after transaction	Tax law, audit, queries	Secure deletion, shredding
Student accommodation records	3 years after end of stay	Queries, references	Secure deletion, shredding
Student support records (extenuating circumstances, reasonable accommodations, pastoral)	7 years after completion	Legal claims, references, documentation	Secure deletion (highly confidential), shredding
Safeguarding records (child protection concerns)	Indefinite or very long term (consult Children First guidance, typically until child reaches 25+ years, or indefinite if serious)	Legal obligation, safeguarding concerns may be relevant decades later	Retained indefinitely; if eventual disposal, consult legal advice and shred securely
Student complaints and appeals records	7 years after resolution	Legal claims, accountability	Secure deletion, shredding
Student consent records (marketing, photographs)	Until consent withdrawn, or 3 years of inactivity	Demonstrating consent obtained; if student withdraws or inactive, no longer need	Secure deletion
Student communications (emails, letters)	Varies: If routine, delete after matter resolved; if significant, retain with student record for 7 years	Depends on significance	Secure deletion, shredding
STAFF DATA			
Staff employment records (contracts, job applications, references, qualifications, Garda vetting)	7 years after employment ends	References, queries, legal claims	Secure deletion, shredding

Staff payroll records (salary, tax, PRSI, bank details)	7 years after tax year	Tax law	Secure deletion, shredding
Staff performance records (observations, appraisals, CPD)	7 years after employment ends	References, documentation, legal claims	Secure deletion, shredding
Staff disciplinary or grievance records	7 years after case closed	Legal claims, accountability	Secure deletion (confidential), shredding
Staff medical records (if held - sick leave, occupational health)	7 years after employment ends	Legal claims, occupational health	Secure deletion (confidential), shredding
OTHER DATA			
Contracts (with students, staff, suppliers, partners)	7 years after contract ends	Legal claims (statute of limitations 6 years, plus 1 year buffer)	Secure deletion, shredding
Financial records (accounts, tax returns, invoices)	7 years after tax year	Tax law, audit	Secure deletion, shredding
Quality assurance data (student feedback, staff feedback, programme reviews, observation reports)	7 years	QA, inspection, accountability, trend analysis	Secure deletion (if contains personal data), shredding
Complaints and incident records	7 years after resolution	Legal claims, accountability	Secure deletion, shredding
CCTV footage (if used)	30 days (unless incident, then retain relevant footage longer)	Security monitoring; 30 days sufficient for identifying incidents	Automatic overwrite after 30 days (unless preserved for incident investigation)
Website analytics and cookies	Varies by type; consent-based cookies deleted when consent withdrawn or after period of inactivity (typically 1 year)	Website functionality and improvement	Automatic deletion by system
Marketing and communications data (prospective students, newsletter subscribers)	Until consent withdrawn or 3 years of inactivity	Marketing; if individual not engaging for 3 years, no longer interested	Secure deletion

Notes:

- **7 years:** Common retention period balancing legal requirements (6-year statute of limitations for contracts, 6 years for tax records, plus buffer) and minimizing data retention
- **Safeguarding:** Very long or indefinite retention due to nature of safeguarding; concerns may be relevant decades later; consult legal advice

- **Longer retention for historical/archival:** In some cases, may retain data longer for legitimate historical, archival, or research purposes (e.g., school archives, historical records - anonymized where possible)

Responsibility:

- Data Protection Lead maintains retention schedule
- Managers responsible for ensuring data in their areas deleted after retention period
- Periodic review of data and deletion of expired data (annual data cleanse)

15. Data Disposal Procedure

When retention period expired, data securely disposed of.

Procedure:

Step 1: Identify Data for Disposal

Annually (or more frequently if practical):

- Review data holdings
- Identify data that has passed retention period (e.g., in March 2026, identify student records from students who completed programmes in June 2018 or earlier - 7 years ago)
- Create list of data to be deleted

Step 2: Confirm No Legal Hold

- **Before deleting, check:**
- Is data subject to legal hold? (e.g., legal claim ongoing, investigation ongoing, statutory authority requested preservation)
- If legal hold, do NOT delete until hold lifted

Step 3: Secure Disposal

Digital Data:

- Delete files from systems
- Empty Recycle Bin / Trash
- For sensitive data, use secure deletion tools (overwrite data multiple times so not recoverable)
- Remove data from backups (where feasible) or ensure old backups eventually overwritten

Paper Records:

- Cross-cut shred (or incinerate if large volume)
- Use confidential shredding service if needed (ensure service provider is reputable and provides certificate of destruction)

Devices:

- If disposing of old computers, hard drives, phones, etc., data must be securely wiped (not just deleted - use data wiping software, or physically destroy drive)
- IT support or specialist data destruction service

Step 4: Document Disposal

Log disposal:

- What data was deleted (e.g., "Student records for cohorts completing 2017-2018")
- Date deleted
- Method (secure deletion, shredding, etc.)

- Person responsible

Documentation provides accountability (can demonstrate compliance with retention and disposal obligations).

PART H: DATA PROCESSING AGREEMENTS WITH THIRD PARTIES

When third party processes personal data on behalf of ELI Schools, Data Processing Agreement (DPA) required.

16. Identifying Data Processors

- **Data Processor:** Third party that processes personal data on behalf of ELI Schools, under ELI Schools' instructions.

Examples at ELI Schools:

- IT service providers (hosting, cloud storage, software providers)
- Email marketing platforms (Mailchimp, etc.)
- Survey platforms (SurveyMonkey, Google Forms if used for collecting personal data)
- Payroll services (if payroll outsourced)
- External IT support (if they access systems containing personal data)
- Shredding services (if confidential shredding outsourced)
- CCTV monitoring services (if CCTV outsourced)

NOT Data Processors (these are separate data controllers or not processing personal data on our behalf):

Awarding bodies (Cambridge, Trinity, etc.) - they are separate controllers when we share student data with them

University partners - - they are separate controllers when we share student transcripts with them

Tusla, Gardaí - separate controllers when we share safeguarding information

Revenue - separate controller when we submit tax data

Distinction:

- **Processor:** Acts on our instructions, processes data on our behalf for our purposes (we are still controller)
- **Separate Controller:** Processes data for their own purposes (they determine purposes and means)

17. Data Processing Agreements (DPAs)

For each data processor, written Data Processing Agreement must be in place BEFORE they begin processing.

DPA Must Include (GDPR Article 28):

A. Subject Matter and Duration:

- What processing the processor will do
- How long the agreement lasts

B. Nature and Purpose of Processing:

- What data will be processed
- Why (purposes)

C. Type of Personal Data and Categories of Data Subjects:

E.g., "Student contact and academic data; data subjects: students"

D. Obligations and Rights of Controller (ELI Schools):

- ELI Schools determines purposes and means
- ELI Schools can audit processor's compliance
- ELI Schools can terminate if processor breaches

E. Processor's Obligations:

Must:

- Process data only on documented instructions from ELI Schools (not use data for own purposes)
- Ensure confidentiality of persons processing data
- Implement appropriate technical and organizational security measures
- Not engage sub-processors without ELI Schools' authorization
- Assist ELI Schools with data subject rights requests
- Assist ELI Schools with security, breach notification, data protection impact assessments
- Delete or return data at end of services (as instructed)
- Make available information to demonstrate compliance
- Allow and contribute to audits by ELI Schools or auditor

F. Sub-Processors:

- If processor uses sub-processors (e.g., hosting provider uses sub-contractors), must have ELI Schools' consent
- Processor must have same obligations in contracts with sub-processors

G. Security:

- Specific security measures processor must implement

H. Data Breaches:

- Processor must notify ELI Schools of breaches without undue delay

I. International Transfers:

- If processor transfers data outside EEA, appropriate safeguards required (Standard Contractual Clauses, etc.)

J. Liability and Indemnity:

- Liability for breaches
- Indemnity (processor indemnifies ELI Schools for processor's breaches)

18. DPA Implementation Procedure

Step 1: Identify All Processors

Data Protection Lead (with assistance from managers):

- Compile list of all third parties processing personal data on behalf of ELI Schools
- For each processor, identify: What data they process, for what purpose, what systems/services they provide

Step 2: Obtain DPAs

For each processor:

Option A: Use processor's standard DPA

- Many reputable processors (Microsoft, Google, Mailchimp, etc.) provide standard DPAs compliant with GDPR
- Review to ensure meets GDPR Article 28 requirements
- Sign/accept DPA (may be online acceptance)

Option B: Use ELI Schools' template DPA

- If processor doesn't have standard DPA, or if their DPA inadequate, ELI Schools can provide template
- Negotiate and sign

Option C: DPA provisions in main service contract

- DPA provisions can be incorporated into main service agreement rather than separate document
- Ensure all GDPR Article 28 requirements included

Step 3: Document and File

- Signed DPAs filed securely
- List of processors and DPAs maintained by Data Protection Lead
- Included in Records of Processing Activities

Step 4: Monitor Compliance

- Periodic review of processors (are they still providing adequate security and compliance?)
- If processor breaches or concerns arise, investigate and take action (terminate contract if serious)
- If processor reports breach, follow data breach procedure

Step 5: Review and Update

- DPAs reviewed when contracts renewed
- If services change significantly, DPA updated
- If new processor engaged, DPA obtained before processing begins

19. Register of Data Processors

Data Protection Lead maintains register:

Processor	Service Provided	Data Processed	DPA in Place	DPA Date	Review Date	Notes
[IT Provider Name]	IT support and hosting	All data on servers (student, staff, operational)	Yes	01/09/2023	01/09/2026	Standard Contractual Clauses for international transfers
[Payroll Service]	Payroll processing	Staff payroll data	Yes	01/01/2024	01/01/2025	DPA in service agreement

Part I: Training

All staff must understand and comply with data protection. Training essential.

20. Data Protection Training Programme

A. Induction Training (All New Staff):

When: Within first month of employment

Format:

- Online module (if available) OR
- In-person training session OR
- One-to-one training from manager or Data Protection Lead
- **Duration:** 30-60 minutes

Content:

- Introduction to GDPR and data protection
- Why data protection matters
- Types of data at ELI Schools
- GDPR principles
- Staff responsibilities (Policy 10.2)
- Security requirements (passwords, clear desk/screen, email, devices, etc.)
- Confidentiality
- Data breaches (what they are, how to report)
- Data subject rights
- Questions and scenarios

Assessment:

- Quiz or acknowledgment form to confirm understanding

Documentation:

Training completion recorded in staff file

B. Annual Refresher Training (All Staff):

- **When:** Annually (e.g., every September)

Format:

- Online refresher module OR
- Training session at staff meeting
- **Duration:** 20-30 minutes

Content:

- Recap of key principles and responsibilities
- Any policy updates or changes
- Common issues or incidents from past year (learning from mistakes - anonymized)
- Reminders (passwords, email security, reporting breaches, etc.)
- Questions

Documentation:

Completion recorded

C. Role-Specific Training:

For staff with particular data protection responsibilities:

Data Protection Lead:

- Advanced training on GDPR, data protection law, compliance
- May attend external courses, webinars, conferences
- Keeps up to date with developments

Managers:

- Training on data protection management responsibilities
- Handling data subject requests
- Investigating breaches
- Staff awareness

IT Support:

- Training on technical security measures
- Data protection in IT systems

D. Ad Hoc Training:

When needed:

- If new systems or processes introduced (data protection implications explained)
- If breach or incident reveals training gap
- If staff member struggling with compliance

21. Training Records

HR Manager (or Data Protection Lead) maintains training records:

Staff Member	Induction Training Date	Annual Refresher 2023	Annual Refresher 2024	Annual Refresher 2025	Notes
John Smith	15/09/2022	Completed 10/09/2023	Completed 05/09/2024	Due Sept 2025	
Jane Doe	20/01/2024	N/A (not employed)	Completed 05/09/2024	Due Sept 2025	
Mark Jones	10/03/2023	Completed 10/09/2023	Completed 05/09/2024	Due Sept 2025	

Monitoring:

- Managers monitor training completion in their teams
- 100% completion target
- Non-completion followed up (reminders, scheduled sessions, escalation if continued non-compliance)

Part J: Monitoring And Audit

Data protection compliance monitored and audited to ensure policies followed and identify improvements.

22. Monitoring Activities

Ongoing Monitoring:

Data Protection Lead monitors:

- Data subject requests (number, types, response times, outcomes)
- Data breaches (number, types, causes, outcomes)
- Training completion rates
- DPAs in place with all processors

23. Internal Audits

Periodic internal audits of data protection compliance:

- **Frequency:** Annually (or more frequently if issues)
- **Who:** Quality Officer, Data Protection Lead, or external auditor if budget allows
- **Scope:**
- Review of policies and procedures (are they up to date and appropriate?)
- Review of Records of Processing Activities (accurate and complete?)
- Review of privacy notices (provided to all data subjects? Up to date?)
- Review of DPAs (in place with all processors?)
- Review of training records (all staff trained?)
- Review of data subject requests log (handled correctly and within timeframes?)
- Review of data breach log (breaches documented, notifications made, learning implemented?)

Output:

- Audit report with findings (strengths, weaknesses, non-compliance, risks)
- Recommendations for improvement
- Action plan

Follow-up:

- Actions implemented
- Progress monitored
- Next audit checks if actions completed

24. Reporting to Governance

Data Protection Lead prepares periodic reports to Board of Directors and Academic Committee:

Quarterly or Annually (as appropriate):

Report includes:

- Overview of data protection compliance status
- Data subject requests (number, types, outcomes)
- Data breaches (number, types, outcomes, actions taken)
- Training completion rates
- DPAs status
- Audit findings and actions

- Risks and issues
- Emerging developments in data protection law or practice
- Recommendations for Board

Purpose:

- Oversight and accountability
- Board assurance that data protection obligations being met
- Board awareness of risks
- Board approval for resources or significant changes

Part K: Review And Improvement

25. Policy and Framework Review

This framework and policies 10.1, 10.2 reviewed:

Schedule: Biennially (every 2 years) or when:

- Legislation changes (GDPR amendments, new Irish data protection law, guidance from DPC)
- Significant changes to ELI Schools operations (new systems, new types of processing, organizational changes)
- Issues identified (breaches, audit findings, complaints)
- Best practice developments

Review Process:

- Data Protection Lead reviews policies and framework
- Consults with managers, staff, legal advisors if needed
- Identifies updates needed
- Proposes revised policies
- Board of Directors approves revised policies
- Staff informed and trained on changes

26. Continuous Improvement

Data protection compliance continuously improved based on:

- Learning from breaches and incidents
- Audit findings
- Feedback from staff and data subjects
- Developments in technology and security
- Sector best practice
- Guidance from Data Protection Commission

Version	1.0
Date Approved	March 2026
Approved by	Managing Director, Board of Directors
Next Review Date	March 2027

Related legislation, regulation or guidelines:

- General Data Protection Regulation (GDPR) (EU) 2016/679
- Data Protection Act 2018 (Ireland)
- Core Statutory Quality Assurance Guidelines 2016 (QQI)
- Code of Practice for Provision of Programmes of English Language Education to International Learners