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

9.4 IT Security and System Access Control

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 ELI Schools' IT security framework, defining standards for access control, system management, data storage, and device security to protect personal data, organizational information, and system integrity across all technology systems and platforms.

Scope

This policy applies to:

- All staff members at ELI Schools (full-time, part-time, temporary, freelance, volunteers)
- All IT systems and platforms used by ELI Schools
- All organizational data stored on company systems
- All devices (computers, laptops, tablets, phones) issued by or used for ELI Schools business
- All cloud services and applications used by the organization
- All locations and centres

Policy Statement

Commitment to IT Security:

ELI Schools is committed to maintaining robust IT security across all systems and platforms. We recognize that:

- IT systems and data are critical assets requiring protection
- Unauthorized access, data breaches, or system failures can cause significant harm to students, staff, and the organization
- Security is a shared responsibility of all staff and IT administrators
- Access to systems and data must be controlled, monitored, and regularly reviewed
- Compliance with data protection law and organizational policy is mandatory

1. Cloud Storage and OneDrive Governance

Company Files Storage Requirements

Policy Statement:

All organizational files, documents, and data must be stored on company-controlled systems only. Personal devices and personal cloud storage accounts must not be used for storing ELI Schools business files or personal data.

Requirements:

Approved Storage Locations:

- Microsoft OneDrive (company account) – primary file storage
- Teams Shared drives/SharePoint – team collaboration
- Orion School Management System – student and academic data
- Brightbooks – financial data and accounts
- Other company-approved systems only

Prohibited Storage:

- Personal OneDrive accounts (personal Microsoft accounts)
- Personal Google Drive, Dropbox, iCloud, or other personal cloud storage
- Personal email accounts for file attachments
- USB drives or portable storage (except as temporary transfer method with encryption)
- Personal computers or devices (unless authorized and with encryption)
- Uncontrolled file-sharing platforms

Rationale:

- Company-controlled storage enables data protection compliance (backup, security, retention management)
- Personal storage accounts cannot be monitored or secured by organization
- Personal accounts may be subject to personal subscription terms that could result in loss of data
- GDPR compliance requires knowing where personal data is stored

Responsibility:

- **Data Controller:** Manages storage infrastructure, access, security
- **All Staff:** Store all work files on company systems only; do not use personal storage
- **Managers:** Monitor their team's file storage practices; ensure compliance

Department-Specific OneDrive Folders

Structure:

OneDrive is organized by department with separate folders:

- **Academic Folder** – Programme materials, curriculum, teaching resources, student-related documents (teaching staff and academic managers only)
- **Operations Folder** – Operations procedures, facilities, safety, risk management (operations staff only)
- **Finance Folder** – Financial records, budgets, invoices, accounts (finance staff and authorized managers)
- **HR Folder** – Staff records, employment documents, payroll (HR staff and managing director only)
- **Marketing Folder** – Marketing materials, campaigns, agent communications (marketing staff only)
- **General Folder** – Organization-wide information (all staff access)

Access Principles:

- **Need-to-Know:** Staff access only folders relevant to their role
- **Departmental Isolation:** Folders separated by department to restrict cross-departmental access
- **Role-Based:** Access assigned to company email and role within department
- **Temporary Access:** May be granted for specific projects with documented approval and time-limited access
- **No Oversharing:** Avoid broad sharing; limit to specific individuals who need access

Responsibility:

- **Data Controller:** Creates and manages folder structure; assigns access; removes access
- **Managers:** Request access for their team members; monitor their team's folder usage
- **All Staff:** Access only approved folders; do not request or attempt to gain access to unauthorized folders

Access Assignment and Removal

New Staff:	• When new staff member begins employment, Data Controller assigns access to relevant OneDrive folders based on role and department • Access assigned to company email address only • New staff member receives access during IT onboarding
Staff Changes:	• When staff member changes role or department, Data Controller reviews access and adjusts (grants additional, removes unnecessary) • Request submitted by manager; approved by Data Controller
Termination:	• When staff member leaves organization (resignation, dismissal, contract end), Data Controller immediately removes all access to OneDrive and other systems • Files remain accessible to department (stored on company system); individual access revoked • Handover of files to successor or manager completed during offboarding
Process:	• Manager notifies Data Controller of changes • Data Controller verifies information • Access changes implemented in Microsoft 365 (company email system controls OneDrive access) • Confirmation provided to manager • Documented in access log

Sensitive File Protection

Additional Security for Highly Sensitive Files

Policy Statement:

Files containing highly sensitive personal data require additional security measures beyond standard OneDrive access control.

Highly Sensitive Files:

- HR records (employment contracts, performance reviews, disciplinary records, payroll data, tax information)
- Financial accounts and records (detailed financial statements, banking information, creditor records)
- Student safeguarding and child protection records
- Medical or health information
- Legal correspondence or litigation-related files
- Data breach records and incident reports
- Student complaints and appeals containing sensitive information

Additional Security Measures:

Password Protection:

- Files containing sensitive data encrypted with password protection
- Password set by Data Controller or file owner
- Password shared only with authorized individuals through secure method (encrypted email, not in file name or on sticky notes)
- Password changed if file widely shared or if person with password leaves organization

File Encryption:

- Highly sensitive files encrypted at file level (Windows Encryption, 7-Zip with encryption, or similar)
- Encryption key or password securely stored (not accessible to unauthorized persons)

Restricted Access:

- Only necessary staff access (typically: relevant manager, finance manager, HR manager, data controller, managing director)
- Access restricted at folder level PLUS additional file-level password protection

Audit Trail:

- Access attempts logged (if system capability)
- File access monitored by manager and Data Controller

Physical Storage:

- If printed, stored in locked cabinet
- Disposal: Cross-cut shredded or incinerated
- Not left unsecured

Responsibility:

- **Data Controller:** Implements password protection; manages encryption; controls access; audits access
- **Managers:** Request password protection for sensitive files; monitor file access; ensure proper disposal
- **All Staff:** Do not attempt to bypass password protection; do not share passwords; report security concerns

Access Control and Sharing

Data Controller Authority

Data Controller Responsibilities:	• Manages access to all systems (OneDrive, Orion, Brightbooks, Microsoft 365, etc.) • Assigns access based on role and department • Revokes access when no longer needed or on staff termination • Reviews access quarterly (at minimum) • Maintains access control log • Ensures access control aligns with Data Protection Governance Framework
No Self-Service Access:	• Staff cannot modify own access or other staff members' access • Staff cannot reset own passwords without IT support • Requests for access go to Data Controller through manager
Authorization Process:	1. Manager identifies staff member needing access 2. Manager submits access request to Data Controller with: 3. Staff member name and company email 4. Systems/folders requiring access 5. Reason for access (role requirement, project, temporary) 6. Duration (ongoing or time-limited) 7. Approval (manager authorization) 8. Data Controller reviews request against role and need-to-know principle 9. Data Controller approves or denies request 10. Data Controller implements access change 11. Confirmation sent to manager and staff member 12. Access change documented in access log

File Sharing Rules

Files must be shared in a controlled manner that maintains access management and security. Sharing links (rather than email attachments) is the preferred method to ensure access control.

Approved File Sharing Methods:

Method 1: OneDrive Sharing Links (Preferred)

- Data Controller or file owner creates sharing link from OneDrive
- Link type set appropriately:
- **"People You Specify"** – Only individuals explicitly granted access can open link (most secure for sensitive files)
- **"Organization"** – Anyone with company email can open link (for internal organizational documents)
- **"Anyone"** – Avoid for any confidential files (appropriate only for public information)
- Link provided to authorized recipient(s) via email
- Link expires after specified period (recommended 30-90 days)
- Recipient does NOT need to download file, accesses via browser
- Access level set: "View" (read-only) or "Edit" (if editing needed) based on purpose

Benefits:

- Centralized access control (can revoke access without retrieving copies)
- Access logged through OneDrive
- No proliferation of file copies

Method 2: Direct Email Link (If Attachment Necessary)

- If file must be attached to email, use OneDrive embedded link (link to OneDrive version, not file attachment)
- If full file attachment necessary (due to technical requirement):
- Only to authorized recipients
- File encrypted or password-protected
- Recipient instructed to delete after use (not store locally)
- Use sparingly

Method 3: Shared Folders

- Files stored in shared OneDrive folders
- Access to folder controlled by Data Controller
- Recipients access files through shared folder
- Centralized management

Prohibited File Sharing:

- Do NOT email sensitive files as attachments without encryption/password
- Do NOT use personal cloud storage links (Dropbox, Google Drive personal account)
- Do NOT forward files to unauthorized persons
- Do NOT create permanent copies on personal devices
- Do NOT share passwords or access credentials
- Do NOT use public link sharing for confidential files

Rationale:

- Sharing links maintain centralized access control (can be revoked)
- Email attachments proliferate copies; impossible to retrieve or track
- Sharing links enable audit trail and logging
- Links can expire automatically
- OneDrive links maintain security and encryption

Responsibility:

Data Controller: Creates and manages sharing links; sets appropriate access
All Staff: Use sharing links instead of attachments;
Managers: Ensure their team uses appropriate sharing method

Access Revocation

Conditions Triggering Access Revocation:	• Staff member no longer needs access for role • Staff member changes role or department • Staff member on unauthorized leave or suspension • Staff member employment terminated • Seasonal role ends • Project completion • Security breach or misuse of access
Process:	• Manager or Data Controller identifies need to revoke access • Data Controller implements revocation in system • Confirmation of revocation documented • Manager notifies staff member (if role change) • Files remain accessible to authorized staff; individual access removed
Timing:	• Immediate: For security breaches, misconduct, employment termination • Within 1 week: For role changes (after handover and knowledge transfer) • At defined time: For time-limited or seasonal access

System Inventory and Management

Approved IT Systems

Policy Statement:

ELI Schools uses specific, approved IT systems for business operations. All staff must use only approved systems and follow Data Controller management of access and security.

System Inventory:

System	Purpose	Owner/Manager	Users	Data Type
Microsoft 365	Email, calendars, Teams, collaboration	Data Controller	All staff	Communication, scheduling, collaboration
OneDrive	File storage and sharing	Data Controller	Staff (role-based)	All organizational files
Orion	School Management System (student records, attendance, assessment, timetabling)	Data Controller	Teaching staff, managers, operations (role-based)	Student data, academic records
Brightbooks	Financial accounting and bookkeeping	Data Controller	Finance staff, managers (role-based)	Financial data, invoices, accounts

Data Controller Responsibilities for Each System:

- User access management (create accounts, assign permissions, remove access)
- Password policies and resets
- System updates and security patches
- Monitoring and logging
- Backup and disaster recovery
- Vendor management and SLAs
- Security incident response

System Requirements

Microsoft 365 (Email and Collaboration):

- Company email: firstname.surname@elischools.com (or assigned variation)
- Strong password policy enforced
- Multi-factor authentication (MFA) available; recommended for sensitive roles
- Mailbox and OneDrive quotas managed
- Automatic backups
- Spam and malware filtering

OneDrive (File Storage):

- Access managed through Microsoft 365 user accounts
- Role-based folder access
- File versioning (previous versions recoverable)
- Automatic backup and sync
- Sharing controls (links with access restrictions)
- Search and discovery

Orion (School Management System):

- User roles defined by Data Controller
- Role-based data access (teachers see own students; finance staff see financial data; management see all)
- Passwords managed by Data Controller
- Session timeout for security
- Audit log of user actions
- Backup and disaster recovery

Brightbooks (Financial Accounting):

- User accounts managed by Data Controller
- Role-based access (data entry, approvals, reporting, audit)
- Passwords managed
- Audit trail of transactions and changes
- Bank feeds and integrations
- Backup and encryption

Unapproved Systems

Policy:

Staff must NOT use unapproved systems or applications for storing, processing, or sharing ELI Schools data or personal data.

Examples of Unapproved Systems:

- Personal Gmail, Hotmail, Yahoo accounts
- Personal Google Drive, Dropbox, iCloud, etc.
- File-sharing sites (WeTransfer, SendAnywhere, file.io)
- Unvetted collaboration tools
- Unsecured messaging apps (WhatsApp, Signal for business files)
- USB drives or external hard drives (except as temporary encrypted transfer)
- Unauthorized software or applications

Consequences:

- Breach of data protection law
- Organizational data at risk
- Disciplinary action up to dismissal

Exceptions:

- If staff member believes an alternative system is needed, request Data Controller approval
- Data Controller assesses security, compliance, and necessity
- If approved, Data Controller implements with appropriate security measures and access controls

Endpoint and Device Control

Data Controller Authority

Policy Statement:

The Data Controller has authority over all devices used for ELI Schools business, including:

- Company-issued computers, laptops, tablets, phones
- Personal devices used for work (with authorization and security measures)

5.2 Device Inventory and Management

Company-Issued Devices:

- All company devices registered and inventoried
- Device assigned to specific staff member with company email
- Data Controller maintains inventory (device make/model, serial number, assigned user, location, issue date)
- Mobile Device Management (MDM) or similar tools used to manage and secure devices
- Devices tracked for maintenance, updates, and security

Device Assignment and Return:

- New staff member receives device during onboarding with security briefing
- Device configured with:
- Staff member's company email and credentials
- Automatic lock screen (5-10 minutes inactivity)
- Password protection
- Encryption (full disk encryption for laptops)
- Antivirus and security software
- VPN (if applicable for remote working)
- On departure, device returned immediately and wiped/reimaged by Data Controller

Personal Device Use (If Authorized):

- Personal devices used for work only with explicit authorization from Data Controller
- Must be secured:
- Password-protected lock screen
- Automatic lock (inactivity)
- Encryption (if storing company files)
- Antivirus and security software
- No personal data of students or staff stored
- All work files deleted on termination
- Device subject to monitoring or management software (if needed for security)
- Device ownership remains with individual; company not liable for loss or damage

Device Security Requirements

All Devices:

- Password protection: Strong passwords (minimum 8 characters, complexity)
- Automatic lock: After 5-10 minutes of inactivity
- Encryption: Full disk encryption for laptops; encryption for personal devices storing company data
- Updates: Operating system, software, security patches installed promptly
- Antivirus: Active antivirus and malware protection
- Firewalls: Personal firewall enabled
- Two-Factor Authentication (2FA/MFA): Enabled where available (especially for email, cloud services)

Remote Access:

- VPN: Used for remote access to company systems (if available)
- Secure connection: Never use public Wi-Fi for accessing company systems or data

Physical Security:

- Devices not left unattended in public areas
- Devices secured when away (locked in office, locked in vehicle)
- Never left in vehicles overnight
- CCTV may be used to monitor device security in offices

Lost or Stolen Devices

Immediate Actions:

- Staff member reports device loss/theft immediately to Data Controller and manager
- Do NOT delay reporting hoping to recover device
- Data Controller takes immediate action:
- If device has remote management capability: remote wipe activated immediately to erase all data
- If no remote capability: assess data at risk; take protective measures (change passwords, reset email, etc.)
- Police report filed (if theft)
- Insurance claim filed (if covered)
- Incident documented (data breach assessment if personal data on device)

Prevention:

- Devices encrypted so that if lost/stolen, data cannot be accessed without encryption password
- Automatic lock prevents unauthorized access if device left unattended
- Staff trained to secure devices and report loss promptly

Logging And Monitoring

Access Logging

Policy Statement:

All access to company systems is logged for security and accountability purposes.

What is Logged:

- User login/logout (who, when, from where if available)
- File access (who accessed what file, when, what action)
- Administrative actions (password resets, access changes, system changes)
- Failed login attempts
- Unusual activity (multiple failed attempts, access outside normal hours, etc.)
- OneDrive file sharing and link creation
- Orion user actions (data viewed, changes made, assessments submitted)
- Brightbooks transactions and changes

Log Retention:

- Logs retained for minimum 1 year
- Older logs may be archived or deleted per data retention schedule
- Logs available for audit and investigation if needed

Access to Logs:

- Data Controller accesses logs as needed for security monitoring and investigation
- Logs not accessible to individual staff members
- Logs used only for legitimate security and compliance purposes

Quarterly Access Review

Quarterly review of system access ensures that access remains appropriate and secure. Quarterly reviews conducted by Data Controller with support from managers.

Review Process:

Frequency: Once per quarter (suggested: January, April, July, October)

Scope:

OneDrive Access Review:	• List of all staff with OneDrive access • Folders each staff member has access to • Assessment: Is access still needed? Is it appropriate for current role? • Action: Remove unnecessary access; grant new access if needed
Orion Access Review:	• List of all Orion users and their roles • Assessment: Role-based access appropriate? Any access escalation not needed? • Action: Remove unnecessary permissions; update roles if staff changed roles
Brightbooks Access Review:	• Finance staff and their access level (data entry, approval, reporting, audit) • Assessment: Access appropriate for current role? • Action: Remove access for staff who left finance role; update permissions if needed
Microsoft 365 Access Review:	• User accounts active/inactive • Team membership (if using Teams) • Assessment: Are all accounts active and necessary? Should any be disabled? • Action: Disable accounts for staff on extended leave; remove from unnecessary Teams
Device Inventory Review:	• Devices tracked and accounted for • Devices assigned to current staff (or returned if staff departed) • Assessment: Is inventory accurate? • Action: Update inventory; flag missing devices; remove departed staff devices

Responsibility:

- **Data Controller:** Conducts review; prepares quarterly report; implements access changes
- **Managers:** Provide input on team members' access needs; confirm access appropriateness
- **All Staff:** Report if they have access they don't need; request access if needed

Documentation:

- Quarterly access review checklist completed
- Findings documented
- Access changes implemented and recorded
- Report provided to Managing Director and Board (if requested)

Outcomes:

- Removal of unnecessary access (follows least-privilege principle)
- Correction of inappropriate access
- Identification of security gaps
- Confirmation that access remains secure

Business Continuity and Disaster Recovery

Backup and Recovery

Policy Statement:

ELI Schools maintains comprehensive backup and recovery procedures to protect against data loss from hardware failure, cyber-attack, natural disaster, or other incidents.

Systems Backed Up:

System	Backup Frequency	Retention	Recovery Capability
Microsoft 365	Continuous (cloud backup)	90 days (Microsoft retention)	Recover deleted files, restore deleted mailboxes
OneDrive	Continuous (cloud sync)	93 days trash retention	Recover deleted files; version history (30 days)
Orion	Daily	30 days (rolling backup)	Full database recovery; point-in-time restore
Brightbooks	Daily	30 days (rolling backup)	Full database recovery; transaction recovery
Email Archive	Continuous	7 years (compliance)	Email recovery; litigation hold

Backup Location:

- Primary backups: Cloud-based (Microsoft, Orion provider, Brightbooks provider)
- Secondary backups: Offsite encrypted backup (if budget allows)
- Benefits: Protects against local hardware failure, ransomware, physical disaster

Data Recovery Process:

If data loss occurs:

- Incident identified and reported to Data Controller
- Assessment: What data lost? Which system? When?
- Data Controller initiates recovery:
- OneDrive: Restore from version history or recovery file
- Orion: Restore from database backup to point before loss
- Brightbooks: Restore from backup; recover transactions
- Email: Recover from archive; restore deleted mailbox
- Recovery time: Varies by system (usually hours to 1-2 days)
- Restoration verified; data integrity confirmed
- Incident documented; root cause analysis

Ransomware and Cyber Attack Protection

Multiple layers of protection in place to protect against ransomware and cyber-attacks:

Protections:	• Antivirus and malware software on all devices (real-time scanning) • Email filtering (malicious emails detected and removed) • Attachment scanning (suspicious files quarantined) • Link scanning (suspicious links identified) • Multi-factor authentication (prevents unauthorized access even if password compromised) • Automatic backups (so even if files encrypted by ransomware, can be recovered from unencrypted backup) • Security updates and patches (vulnerabilities fixed promptly) • Staff training (phishing awareness, suspicious email recognition, safe browsing)
Incident Response:	• If ransomware suspected: Immediately disconnect affected device from network • Report to Data Controller immediately • Do NOT pay ransom • Restore from unencrypted backup • Investigate how ransomware entered; prevent future incidents

Disaster Recovery Plan

ELI Schools has a documented disaster recovery plan for major incidents (building damage, cyber-attack, extended IT outage, etc.).

Plan includes:	• Identification of critical business functions and systems • Recovery priorities (what must be restored first) • Recovery procedures for each critical system • Communication plan (how to inform staff, students, stakeholders) • Alternate work locations (if building unavailable) • Alternative communication methods (if primary systems down) • Testing of recovery plan (at least annually) • Responsibility assignments
Recovery Time Objectives (RTO):	• Email: 4 hours (business continuity critical) • OneDrive/File Storage: 8 hours • Orion (student management): 24 hours (ideally less) • Brightbooks: 48 hours (less critical for daily operations)
Recovery Point Objectives (RPO):	• Maximum data loss accepted: 1 day (all systems have daily backups)
Business Continuity:	• Plans in place to continue essential operations if IT systems down (manual processes, alternate locations, alternate staff) • Staff trained in business continuity procedures

Compliance And Responsibilities

Compliance with Policy

All Staff Must:	• Store company files on company systems only (OneDrive, Orion, Brightbooks, approved systems) • Do NOT use personal cloud storage, personal email, or unapproved systems for company data • Access only systems and files authorized for their role • Use sharing links (not attachments) for sharing files • Protect passwords and devices • Report security concerns or breaches immediately • Complete IT security training • Follow Data Controller's instructions on access and device management
Managers Must:	• Ensure their team stores files on company systems • Request access changes for their team through proper channels • Monitor their team's compliance with IT security policy • Report non-compliance to Data Controller and Managing Director
Data Controller Must:	• Manage and grant access to all systems and files • Conduct quarterly access reviews • Maintain system security (updates, patches, antivirus, firewalls) • Implement backups and disaster recovery • Investigate security incidents • Maintain access logs • Report to Board on security status

Violations and Consequences

Policy Violation Examples:	• Storing company data on personal cloud storage • Sharing files as email attachments instead of links (for sensitive data) • Unauthorized access to systems or files • Sharing passwords or access credentials • Leaving devices unsecured • Not reporting data breaches or security concerns • Disabling security features • Installing unapproved software
Consequences:	• First violation: Warning and retraining • Repeated violation: Formal disciplinary action • Serious violation (intentional breach, data theft, etc.): Suspension or dismissal • Loss of access to systems • Legal action if criminal
Training and Awareness	• IT Security Induction training: Passwords, devices, file storage, phishing awareness, incident reporting (within first month) • Annual IT Security Refresher training • Specific training for systems used in their role (Orion, OneDrive, Brightbooks)

School Management System (Orion)

Overview

ELI Schools operates a bespoke, in-house learner management system called **Orion**, purpose-built to meet the specific needs of our multi-centre English language education provision. Orion is designed to integrate all aspects of learner management, from initial inquiry through to programme completion and beyond, while maintaining secure, role-based access controls and data protection compliance.

The Orion system serves as the central hub for all operational, academic, administrative, financial, and marketing functions across all ELI Schools centres. It enables efficient data management, real-time reporting, and informed decision-making while ensuring appropriate data security and privacy protections.

System Principles

The Orion system is designed around the following core principles:

Role-Based Access: All users have secure, restricted access to system features based on their job role and responsibilities. Users can only access information and features necessary for their role.

Data Security: The system incorporates multi-level security controls, encryption, and audit trails to protect sensitive learner, financial, and operational data.

Data Controller Governance: A designated Data Controller manages, and controls user access, feature availability, and data permissions based on individual role requirements.

Integration: All system modules are fully integrated, enabling seamless data flow and consistency across the organization.

Real-Time Reporting: Live data feeds enable accurate, up-to-date reporting and decision-making.

Efficiency and Accuracy: Automated processes, pre-built reports, and data validation minimize manual errors and save time.

Training and Support: Comprehensive training manuals and user guides support all staff in using system features appropriate to their roles.

Orion represents a significant investment in operational efficiency, data security, and quality assurance for ELI Schools. Through role-based access, secure data controls, comprehensive feature sets, and integrated reporting, Orion enables all staff to perform their roles effectively while maintaining appropriate security and privacy protections for learner data. Ongoing training, support, and governance ensure that Orion continues to meet organizational needs and regulatory requirements.

System Modules and Features

Management Dashboard

Purpose

The Management Dashboard provides senior leadership and academic management with a real-time overview of operational status across all three ELI Schools centres, enabling effective capacity planning and resource allocation.

Access

- **Senior Management** (Academic Director, Board of Directors)
- **Academic Compliance Management** (Academic Manager)

Key Features

Centre Occupancy and Capacity:

- Current learner arrivals by centre
- Current learner departures by centre
- Total occupancy for each centre (morning and afternoon sessions)
- Overall capacity utilization percentage
- Capacity forecasting and planning tools

Classroom Occupancy:

- Current classroom usage (morning and afternoon)
- Classroom availability and utilization
- Classroom status and equipment functionality
- Timetabled vs. actual occupancy

Staffing Overview:

- Teacher availability and allocation
- Substitute teacher requirements
- Academic management coverage
- Administrative staff status

Planning Tools:

- Capacity planning for future enrolment
- Class composition and balance planning
- Teacher and staff requirement forecasting
- Operational resource planning

Use Cases

Senior management uses the Management Dashboard to:

- Monitor daily centre operations across locations
- Identify capacity constraints and plan solutions
- Forecast staffing and resource requirements
- Make strategic decisions on course scheduling and pricing
- Ensure equitable distribution of learners and resources across centres

Academic Module

Purpose

The Academic module provides comprehensive access to all learner academic information and tools for managing teaching, learning, assessment, and learner progression.

Access

- **Director of Studies**
- **Assistant Director of Studies**
- **Academic Manager**

Key Features

Learner Academic Profiles:

- Complete academic history and progress
- Current level and programme
- Learning outcomes achievement
- Assessment results and grades
- Examination performance and certifications
- Notes and observations from teachers

Learner Personal Profiles:

- Learner contact information
- Emergency contact details
- Special needs and accommodations
- Health and medical information
- Learning preferences and styles
- Goals and aspirations

Class Management:

- Class lists and rosters
- Class composition and balance
- Class schedule and timetable
- Class resources and materials allocation
- Class notes and progress tracking

Classing and Placement Tools:

- Learner placement algorithms
- Level placement and testing
- Class allocation and assignment
- Class changes and movements
- Progression tracking between levels

Attendance Management:

- Attendance recording (daily)
- Absence recording and authorization
- Attendance reports and analytics
- Late arrival and early departure logging
- Attendance patterns and trends

Level Changes and Progression:

- Level change requests and approvals
- Progression criteria and tracking
- Level change documentation
- Student communication on level changes
- Historical progression records

Academic Module
Continued

Examination Management:

- External examination bookings and registrations
- Examination schedules and timetables
- Examination results and performance analysis
- Certification and results distribution
- Examination preparation tracking

Teacher Profiles and Performance:

- Teacher qualifications and credentials
- Teaching schedule and allocation
- Observation records and feedback
- Performance evaluations
- Professional development history
- Training completion and certifications

Classroom Management:

- Classroom availability and booking
- Classroom resources and equipment
- Classroom maintenance and issues
- Room allocation and optimization
- Capacity and utilization tracking

Reporting Tools:

- Real-time academic dashboards
- Learner progress reports
- Class performance reports
- Attendance and retention analytics
- Achievement and outcome reports
- Teacher workload and performance reports
- Examination results analysis
- Custom report generation

Use Cases

Academic staff use the Academic module to:

- Manage daily teaching operations and classes
- Monitor learner progress and identify concerns
- Track attendance and address absences
- Manage learner level changes and progression
- Organize examination bookings and results
- Prepare reports for stakeholders
- Ensure compliance with quality assurance requirements
- Make informed decisions on teaching and learning improvements

Admissions Module

Purpose

The Admissions module manages the complete learner journey from initial inquiry through enrolment, including bookings, services, pricing, payments, and confirmation documentation.

Access

- **Admissions Staff**
- **Administrative Manager**
- **Academic Director** (reporting and analysis features)

Key Features

Learner Profiles (Admissions View):

- Inquiry and booking history
- Services requested and selected
- Pricing and quotations
- Payment history and status
- Invoices and payment records
- Confirmation documents

Booking Management:

- Inquiry capture and recording
- Booking creation and modification
- Service selection and packaging
- Pricing and fee structure application
- Quotation generation
- Booking confirmation

Services Management:

- Available services and options
- Programme selection
- Accommodation selection
- Transfer services
- Additional services (e.g., examination preparation, one-to-one tuition)
- Service pricing and add-ons

Payment Management:

- Payment processing and recording
- Payment plans and schedules
- Payment status tracking
- Refunds and cancellations
- Payment confirmations
- Financial reporting integration

Invoice Management:

- Automatic invoice generation
- Invoice customization
- Invoice sending and tracking
- Invoice payment tracking
- Late payment reminders
- Cancellation and adjustment processing

Confirmation Documents:

- Automated generation of confirmation letters
- Booking condition acceptance
- Programme and service details
- Payment terms and conditions
- Learner acceptance and acknowledgment

Admissions Module
Continued

Reporting Tools:

- Booking pipeline reports
- Arrival forecasting
- Payment status reports
- Services requested analysis
- Cancellation and refund tracking
- Revenue forecasting

Use Cases

Admissions staff use the Admissions module to:

- Process new learner inquiries efficiently
- Generate quotes and booking confirmations
- Manage booking modifications and cancellations
- Track payments and send reminders
- Generate and send confirmation documents
- Report on booking pipeline and arrivals
- Forecast revenue and staffing requirements

Accommodation Module

Purpose

The Accommodation module manages all aspects of learner accommodation, from host family recruitment and vetting through to booking, occupancy management, and performance monitoring.

Access

- **Accommodation Manager**
- **Administrative Manager** (reporting features)

Key Features

Host Family Profiles:

- Host family information and contact details
- Application and interview records
- Police vetting and reference checks
- Home inspection reports
- Profile assessment and suitability
- Profile status (active, inactive, vetted, etc.)

Accommodation Provider Profiles:

- Residence/accommodation provider information
- Contact and emergency details
- Agreement and contract details
- Vetting and compliance status
- Quality standards and compliance

Host Family Management:

- Application processing and tracking
- Vetting and police check coordination
- Home inspection scheduling and recording
- Profile updates and amendments
- Status management (application, vetted, active, inactive)
- Removal from service (with reasons)
- Performance monitoring and ratings

Accommodation Module

Accommodation Bookings:

- Booking creation and assignment
- Learner-accommodation matching
- Booking confirmation and changes
- Cancellation and adjustments
- Special requirements recording (dietary, medical, accessibility)
- Payment and invoicing integration

Booking Confirmations and Link Tracking:

- Automated booking confirmation emails
- Learner acceptance links
- Host family acceptance and acknowledgment
- Booking condition acceptance tracking
- Link engagement analytics

Occupancy and Capacity Management:

- Real-time occupancy tracking
- Available rooms and capacity
- Occupancy forecasting
- Waiting lists and allocation
- Capacity utilization reporting
- Seasonal demand patterns

Performance Management:

- Learner reviews and ratings of accommodation
- Host family feedback collection
- Quality issue tracking and resolution
- Performance dashboards
- Accommodation quality reports
- Issue resolution tracking

Arrival Pipeline Management:

- Upcoming arrivals calendar
- Accommodation assignment timeline
- Payment status tracking
- Confirmation status
- Special requirements preparation
- Contingency planning for non-confirmed bookings

Reporting Tools:

- Occupancy reports and forecasts
- Performance and quality reports
- Issues and complaints tracking
- Learner satisfaction reports
- Host family performance analytics
- Revenue and payments reporting

Use Cases

Accommodation staff use the Accommodation module to:

- Recruit and vet new host families
- Manage accommodation bookings and assignments
- Track learner arrivals and placements
- Monitor accommodation quality and performance
- Address issues and complaints
- Report on capacity and occupancy
- Ensure timely and appropriate placements

Finance Module

Purpose

The Finance module provides comprehensive financial management, including payments, invoicing, income tracking, expenses, and financial reporting across all revenue streams and cost centres.

Access

- **Finance Manager**
- **Administrative Manager** (reporting features)
- **Academic Director** (reporting features)

Key Features

Learner Payment Management:

- Learner payment profiles and history
- Payment recording and tracking
- Payment method management
- Payment reconciliation
- Payment status and arrears tracking
- Refunds and credits

Income Management:

- Learner fee income tracking
- Income by programme, course type, and centre
- Income forecasting and reporting
- Cancellation and refund recording
- Revenue recognition and reporting

Expense Management:

- Expense recording and categorization
- Vendor and supplier management
- Expense approvals and authorization
- Expense reporting and analysis
- Budget vs. actual tracking

Specialized Payment Processing:

- **Visa and Escrow Payments:** Separate tracking for visa-related escrow accounts
- **Examination Payments:** Recording of examination payments with exam board reference codes
- **Medical Insurance Payments:** Recording of medical insurance payments with reference codes and invoice tracking
- **PEL (Points English Language) Payments:** Tracking with reference codes (if applicable)
- **Host Family Payments:** Separate host family payment processing and reporting

Invoicing and Billing:

- Automatic invoice generation
- Invoice customization and templates
- Invoice distribution and tracking
- Payment tracking against invoices
- Aging analysis and arrears management
- Late payment reminders and follow-up

Finance Module
Continued

Journals and Transactions:

- General ledger journal entries
- Transaction recording and categorization
- Transaction audit trail and history
- Reconciliation of transactions

Host Family Payment Reports:

- Host family payment processing
- Payment schedules and amounts
- Payment confirmations
- Payment history and records
- Reconciliation reporting

Financial Reporting and Analysis:

- Income and expense reports
- Profit and loss reporting
- Cash flow analysis
- Budget variance analysis
- Financial dashboards
- Centre-by-centre financial reporting
- Programme-level financial analysis
- Year-on-year comparisons

Reconciliation Features:

- Bank reconciliation
- Payment reconciliation
- Expense reconciliation
- Revenue reconciliation
- End-of-period reconciliation

Use Cases

Finance staff use the Finance module to:

- Record and track all learner payments
- Generate invoices and manage payments
- Process refunds and cancellations
- Track specialized payments (visa, exams, insurance, host families)
- Reconcile accounts and transactions
- Generate financial reports for management and stakeholders
- Monitor budget vs. actual performance
- Forecast future revenue and expenses

Marketing Module

Purpose

The Marketing module manages learner bookings, agent relationships, agent performance, and price lists, supporting marketing strategy and sales analysis.

Access

- **Marketing Manager**
- **Administrative Manager** (reporting features)

Key Features

Learner Bookings (Marketing View):

- Booking source and channel tracking
- Booking data for marketing analysis
- Learner demographics and origin
- Booking trends and patterns
- Conversion tracking

Agent Profiles:

- Agent information and contact details
- Agency details and representation
- Agent agreements and contracts
- Commission rates and payment terms
- Contact person details
- Agent status (active, inactive, pending)
- Rating and performance classification

Agent Performance Tracking:

- Bookings by agent
- Revenue generated by agent
- Conversion rates and pipeline
- Performance trends and analytics
- Agent comparison and benchmarking
- Performance-based commissions and payments

Agent Application and Management:

- Agent application process
- Application review and approval
- Contract negotiation and execution
- Profile setup and configuration
- Agent onboarding
- Profile updates and amendments
- Status changes and removal

Price Lists:

- Current price list management
- Price list version control
- Price by programme and service
- Seasonal pricing adjustments
- Agent-specific pricing (if applicable)
- Price list distribution and access
- Price list history and changes

Marketing Module
Continued

Sales Reporting and Analysis:

- Sales by agent, region, country
- Sales by course type and duration
- Sales trends and forecasting
- Market analysis and segmentation
- Regional performance reports
- Country-level analysis
- Revenue tracking by source
- Learner origin and demographic analysis
- Custom sales reports with multiple filters

Use Cases

Marketing staff use the Marketing module to:

- Track and manage agent relationships
- Monitor and analyse sales performance
- Identify high-performing agents and markets
- Forecast revenue and pipeline
- Manage and update price lists
- Generate sales reports for management
- Support strategic marketing decisions

Documents Module

Purpose

The Documents module provides secure management of document templates and master files used throughout the organization, with controlled access and version management.

Access

- **Document Administrator** (assigned staff with document management responsibilities)
- **Other staff members** (read-only access to required documents based on role)

Key Features

Master Document Repository:

- Centralized storage of all document templates
- Document categorization and organization
- Document version control and history
- Current version tracking and identification
- Archived versions retained for records

Document Categories:

- Learner confirmation and enrolment documents
- Invoices and billing documents
- Accommodation confirmations and agreements
- Booking confirmations and details
- Certificates and achievements
- Reports and analytics outputs
- Policy and procedure documents
- Marketing and promotional materials
- Financial and payment documents
- Legal and compliance documents

Documents Module
Continued

Document Management Features:

- Document creation and upload
- Version control and version history
- Document updates and amendments
- Approval workflows (where required)
- Release and deployment of updated documents
- Archive and retrieval of superseded versions
- Usage tracking and deployment monitoring

Document Updates and Maintenance:

- Regular review of templates
- Updates for changes in policies, fees, or conditions
- Changes communicated to relevant staff
- Training on template use and updates
- Quality assurance of document content
- Consistency checks across related documents

Access Control:

- Role-based access to documents
- Read-only access for most staff
- Edit access restricted to designated administrators
- Audit trail of document access and downloads
- Secure storage and encryption

Document Deployment:

- Integration with other Orion modules for automatic document generation
- Mail merge and customization features
- Document tracking and delivery
- Recipient acknowledgment and acceptance
- Document archiving and retrieval

Use Cases

Document administrators use the Documents module to:

- Create and maintain document templates
- Update templates with policy, fee, or condition changes
- Deploy updated templates to system users
- Control access to sensitive documents
- Maintain version history for compliance
- Support consistent communication with learners and stakeholders

Other staff members use the Documents module to:

- Access required templates and documents
- Download and print documents as needed
- View current versions and understand recent changes
- Retrieve archived versions when necessary

Security and Access Control Module

Purpose

The Security and Access Control module provides data governance and user access management, ensuring appropriate role-based access, data security, and compliance with data protection requirements.

Access

- **Data Controller** (designated senior staff member responsible for data protection)
- **System Administrator** (technical user management)

Key Features

User Management:

- User account creation and provisioning
- User profile and role assignment
- Job title and department tracking
- Start and end dates for employment
- User status (active, inactive, suspended)
- User account termination and deletion

Role Definition and Management:

- Pre-defined roles aligned to job positions
- Custom role creation where required
- Role descriptions and permission definitions
- Role hierarchy and relationships
- Role updates and amendments
- Obsolete role retirement

Feature-Based Access Control:

- Feature assignment to roles
- Module-level access (Academic, Admissions, Finance, etc.)
- Feature-level permissions within modules
- Read, write, delete permissions
- Approval and workflow permissions
- Report access and customization

Data Access Restrictions:

- Centre-level restrictions (access to specific centres only)
- Learner-level restrictions (access to specific learner records)
- Financial-level restrictions (access to financial data)
- Sensitive data masking (e.g., credit card information)
- Department-level restrictions
- Custom data restrictions as needed

Sensitive Data Access Controls:

- Restricted access to payment information
- Restricted access to personal/medical information
- Restricted access to financial data
- Restricted access to safeguarding information
- Audit logging of sensitive data access
- Additional authentication for sensitive data access

Security and Access Control Module
Continued

Data Controller Responsibilities:

- Review and approve user access requests
- Assign appropriate roles and permissions
- Monitor unusual access patterns or activities
- Manage data protection compliance
- Review and update access policies
- Handle access request denials and appeals
- Ensure least-privilege principle applied
- Regular access audits and reviews

Access Governance:

- Access request and approval workflows
- Periodic access reviews (quarterly/bi-annually)
- De-provisioning of inactive users
- Immediate de-provisioning of leavers
- Segregation of duties to prevent conflicts of interest
- Exception management and escalation

Audit and Logging:

- User login and activity logging
- System change audit trail
- Data access logging
- Sensitive data access recording
- Failed access attempt logging
- Compliance reporting and audit trails
- Log retention and archiving

Security Features:

- Password policies and management
- Multi-factor authentication (where appropriate)
- Session management and timeouts
- Encryption of data in transit and at rest
- IP address restrictions (where applicable)
- Antivirus and security updates
- System vulnerability management

Compliance Monitoring:

- GDPR compliance monitoring
- Data access compliance
- Data retention compliance
- Third-party access management (if applicable)
- Regulatory reporting capabilities
- Internal audit support

Use Cases

The Data Controller uses the Security and Access Control module to:

- Create new user accounts and assign roles
- Update user roles as responsibilities change
- Remove access for leavers or transferred staff
- Grant additional permissions for new initiatives
- Monitor access patterns for security issues
- Conduct periodic access reviews
- Ensure data protection and GDPR compliance

Support internal and external audits

Data Governance and Responsibilities

Data Controller Role

A designated Data Controller is responsible for:

- Overseeing all user access and permissions
- Ensuring appropriate role-based access controls
- Managing data protection and GDPR compliance
- Reviewing and approving access requests
- Monitoring system security and audit trails
- Ensuring least-privilege principal compliance
- Conducting periodic access reviews
- Managing system backups and disaster recovery
- Reporting on data governance matters to management

The Data Controller is typically:

- The Academic Director, or
- A designated senior management team member with specific responsibility for data governance

Responsibility of All Users

All staff using Orion are responsible for:

- Understanding their role and permitted access
- Protecting their login credentials
- Not sharing access credentials
- Logging out after use
- Reporting security concerns immediately
- Following data protection policies
- Not accessing data outside their role requirements
- Completing system training and security updates
- Understanding safeguarding and confidentiality requirements

Training and Support

System Training

Comprehensive training is provided for all Orion modules and features:

Training Coverage:

- Departmental training manuals for each module
- Role-specific training for each user group
- Process-specific training for key procedures
- New starter induction training
- Update training when features change
- Ongoing support documentation and FAQs

Training Delivery:

- Initial in-person or online training for new users
- Self-service training materials and guides
- Troubleshooting guides and FAQs
- Video tutorials for complex processes
- Regular refresher training
- Support and mentoring from experienced users

Training Responsibility:

- System Administrator coordinates training scheduling
- Department managers ensure staff complete training
- All new staff complete system training within first week
- Staff update training completed within one week of system changes

User Support

Ongoing support is provided through:

- Help desk ticketing system
- FAQ documentation and knowledge base
- Video tutorials and demonstrations
- Direct support from System Administrator
- Escalation procedures for complex issues
- Regular user feedback and system improvement

System Maintenance and Updates

Regular Maintenance

- Database backups (daily)
- Security patches and updates (as released)
- Performance monitoring and optimization
- Data integrity checks and validation
- Archive of inactive/old data

System Updates and Enhancements

- Updates communicated to users in advance
- Training provided for significant changes
- Phased rollout to minimize disruption
- User feedback incorporated into improvements
- Change logs and documentation maintained

Online File Records and OneDrive File Management

ELI Schools uses Microsoft OneDrive as a centralized platform for organizing, storing, and managing organizational files and records. OneDrive provides secure cloud-based storage with controlled access, version control, and collaboration features that support departmental workflows while maintaining appropriate data security and privacy protections.

The OneDrive system complements the Orion learner management system by providing secure storage for documents, records, policies, templates, and departmental files that support daily operations across all ELI Schools centres.

OneDrive System Principles

The OneDrive file management system operates according to the following principles:

- **Role and Department-Based Organization:** Files and folders are organized by role and department to enable efficient access to relevant information.
- **Controlled Access:** Access to all folders is controlled and restricted based on job role and departmental responsibilities. Users can only access folders necessary for their role.
- **Data Controller Governance:** A designated Data Controller manages all folder access, permissions, and user assignments. Access changes can be applied remotely without employee input or action.
- **Security and Privacy:** File access, sharing, and permissions are configured to protect sensitive organizational and learner data.
- **Version Control:** OneDrive's built-in version history enables tracking of changes and recovery of previous file versions.
- **Collaboration:** OneDrive enables secure collaboration within authorized teams while maintaining access restrictions.
- **Backup and Recovery:** Cloud-based storage provides automatic backup and recovery capabilities.

Folder Structure and Organization

OneDrive Folder Hierarchy ELI Schools maintains the following role and department-based folder structure:

Academic Folders:	• **Academic Quality:** Teaching quality, lesson observations, professional development, curriculum materials, teaching standards, and best practices documentation • **Academic Compliance:** QA Manual compliance tracking, internal audits, self-evaluation reports, quality assurance procedures, and compliance monitoring records
Support Services Folders	• **Accommodation:** Host family profiles and vetting documents, accommodation agreements, inspection reports, performance records, and occupancy management files • **Safeguarding:** Child protection policies and procedures, safeguarding incident records, training records, welfare documentation, and designated person contact information • **Student Experience:** Social programme documentation, cultural activities, events planning, learner feedback, and engagement initiatives
Administrative Folders:	• **Reception:** Reception procedures, visitor management, emergency contacts, reception schedule, and administrative processes • **Forms and Templates:** Master copies of all organizational forms, templates, letterheads, and document templates used across the organization
Marketing and Sales Folders:	• **Marketing:** Marketing campaigns, promotional materials, branding guidelines, advertising materials, and marketing strategy documentation • **Sales and Invoices:** Sales records, invoice templates, payment documentation, financial records, and sales performance data • **Groups and Juniors:** Junior programme documentation, group booking records, group-specific materials, and junior learner information
Learner Record Folders:	• **Student Documents:** Learner application forms, verification documents, enrolment documentation, correspondence with learners, and learner-specific records • **PEL and Insurance:** PEL (Points English Language) documentation and reference codes, medical insurance information, insurance claims, and related records
Admissions Folder:	• **Admissions:** Booking confirmations, learner inquiries, admission documentation, pre-arrival information, and admissions process records
Compliance and Safety Folders:	• **Safety Management:** Health and safety documentation, incident reports, emergency procedures, risk assessments, fire safety records, and safety committee minutes • **Safeguarding:** (As described above) Child protection and welfare documentation
Financial and HR Folders:	• **Accounts:** Financial records, expense documentation, invoicing, payment records, financial reports, and accounting documentation • **HR:** Staff recruitment files, employment contracts, personnel records, disciplinary records, performance reviews, staff training records, and HR documentation
Training and Resources:	• **Training Manuals:** Training materials for all systems and processes, Orion user manuals, departmental procedures, policy guides, and staff development resources

Access Control and Permissions

Access Management

All OneDrive folder access is:

- **Controlled by the Data Controller:** The designated Data Controller manages all folder access and permissions
- **Role-Based:** Users have access to folders relevant to their job role and responsibilities
- **Department-Based:** Users have access to their department's folders and shared cross-departmental folders as needed
- **Regularly Reviewed:** Access is reviewed periodically to ensure it remains appropriate
- **Remotely Managed:** The Data Controller can change or revoke access remotely without requiring employee action

Default Access by Role

Academic Management (Director of Studies, ADOS):

- Academic Quality
- Academic Compliance
- Groups and Juniors
- Student Documents (viewing only)
- Safeguarding (as appropriate)
- Training Manuals

Teaching Staff:

- Academic Curriculum content only

Accommodation Manager:

- Accommodation
- Student Documents (accommodation-related)
- Forms and Templates
- Training Manuals

Welfare Officer:

- Student Experience
- Accommodation
- Student Documents
- Forms and Templates
- Training Manuals

Reception/Administrative Staff:

- Reception
- Forms and Templates
- Student Documents (general access)
- Training Manuals
- (Additional access based on specific role)

Marketing Manager:

- Marketing
- Sales and Invoices
- Groups and Juniors
- Forms and Templates
- Training Manuals

Default Access by Role	**Admissions Staff:** • Admissions • Student Documents • Sales and Invoices • Forms and Templates • PEL and Insurance • Training Manuals **Finance Staff:** • Accounts • Sales and Invoices • PEL and Insurance • Forms and Templates • Training Manuals **Designated Laision Person:** • Safeguarding **HR Manager:** • HR • Forms and Templates • Training Manuals **Senior Management:** • All folders (full access)

Access Request and Changes

New Users:	• Access folders assigned based on job role • Data Controller configures access during onboarding • Access configured within first week of employment • User receives notification of available folders
Role Changes:	• Employee's manager notifies Data Controller of role change • Data Controller updates folder access accordingly • Previous role's folders removed from access • New role's folders added to access • User receives notification of access changes
Additional Access Requests:	• Employee requests additional folder access from manager • Manager approves/denies request • If approved, Data Controller configures access • Data Controller notifies user of access changes
Access Removal:	• For departing staff: Access removed on final working day • For role changes: Old role's access revoked immediately • For security concerns: Data Controller can revoke access immediately • User receives notification of access changes

Sensitive Data Restrictions

Certain folders have additional access restrictions:

Safeguarding Folder:	• Access restricted to designated safeguarding personnel • Additional folders for named designated persons only • Restricted access to incident records • Audit logging of all access
HR Folder:	• Access restricted to HR personnel and Senior Management • Personnel records folder restricted to HR staff only • Disciplinary and performance records restricted access • Audit logging of all access
Accounts Folder:	• Access restricted to Finance staff and Senior Management • Sensitive financial records with restricted access • Payment and banking information restricted access • Audit logging of all access
PEL and Insurance Folder:	• Restricted access to admissions and finance staff • Payment reference codes and sensitive data restricted • Medical information restricted to authorized staff • Audit logging of all access

File Organization and Management

Folder Organization Standards

All OneDrive folders follow standardized organizational practices:

Naming Conventions:	• Clear, descriptive folder and file names • Consistent naming structure within departments • Date formatting (DD-MM-YYYY) for dated files • Consistent abbreviations and codes
Subfolder Structure:	• Logical organization within department folders • Consistent subfolder hierarchy across similar departments • Archive folders for old or inactive files • Templates and forms organized in separate subfolders
File Naming:	• Descriptive file names indicating content and date • Consistent formatting and structure • Version numbers for document versions • Status indicators (draft, final, approved) where appropriate
File Organization:	• Current files in main folders • Archive subfolders for inactive or historical files • Templates in designated templates subfolders • Draft files in clearly marked draft folders

Document Version Control

OneDrive's built-in version control features include:

Version History

- Automatic saving of previous versions
- Access to version history for all files
- Ability to restore previous versions
- View changes by date and user
- Comments and change tracking

File Sharing and Collaboration:

- Co-authoring features for collaborative editing
- Comments and version notes
- Change tracking and highlighting
- Reconciliation of concurrent edits

File Retention and Archive

Active Files:

- Current files stored in main department folders
- Regularly accessed and updated files
- Working files and in-progress documents

Archive Files:

- Files no longer in active use moved to archive subfolders
- Historical records and completed projects
- Retention in archive for required periods
- Clear dating and labelling of archived files

Deletion Policies:

- Deletion only by Data Controller authorization
- Backup of deleted files maintained where required
- Audit trail of deletions
- Compliance with data retention policies

File Access and Sharing Protocols

Within Departments:

Internal Sharing

- Files shared within department folders automatically
- Shared access based on departmental folder permissions
- No additional sharing authorization required

Cross-Departmental Sharing:

- Controlled sharing between departments
- Data Controller approval for cross-departmental access
- Access configured through folder permissions
- Temporary access revoked after specified period if needed

Individual Sharing:

- Limited individual file sharing within organizational folders
- File sharing logged and monitored
- Sensitive files not shared individually
- Team-based access preferred over individual sharing

External Sharing

External Sharing Policy:
- External sharing of OneDrive files is generally restricted
- External sharing only with explicit Data Controller approval
- Limited to specific, business-critical circumstances
- Access links include expiration dates where appropriate
- Audit logging of all external sharing

Authorized External Sharing:
- Limited circumstances where external sharing is permitted:
  - Sharing documents with education agents (specific file types only)
  - Sharing marketing materials with external partners
  - Sharing policy documents with regulatory bodies
  - Sharing learning resources with learners (in specific contexts)

Access Controls for External Sharing:
- Expiring links for temporary access
- View-only access (no download or edit)
- Password protection for sensitive documents
- Audit tracking of external access and downloads
- Ability to revoke access immediately

Data Security

Access Controls:
- Role-based access controls
- IP restrictions where appropriate
- Multi-factor authentication for sensitive access
- Session timeouts and forced re-authentication

Audit Logging:
- Logging of all file access and downloads
- Tracking of file modifications and changes
- User identification for all actions
- Retention of audit logs for compliance

Backup and Recovery:
- Automatic cloud-based backup
- Version history recovery
- Disaster recovery capabilities
- Data redundancy for business continuity

Training and Support

OneDrive Training

All staff receive training on:
- OneDrive access and navigation
- Folder structure and organization
- File naming and organization standards
- Sharing and collaboration features (where appropriate)
- Data protection and confidentiality requirements
- Reporting security concerns

New User Onboarding

New staff complete OneDrive training during induction:
- Access to assigned folders confirmed
- Folder structure and content explained
- Key files and resources identified
- Questions and support provided
- Follow-up available for additional support