Data Protection, Information Governance and Security Policy

Purpose: To provide one clear framework for data protection, information governance and security across Future Projects, with the additional arrangements and privacy information required for Future Education in the same document.

Including the Future Education supplement and privacy notices

Applies to	All Future Projects services and functions, including Future Education, Future Support, Future Radio, central functions, premises, outreach, remote work and new or renamed services. Parts B and C contain the additional arrangements and privacy notices for Future Education.
Document control	**Details**
Document owner and Data Protection Officer	Laura Knight, Finance & Business Support Officer – organisational Data Protection Officer (DPO) and Data Protection Lead (DPL)
Technical security lead	IT Manager
Executive approval	Daniel Childerhouse, Chief Executive Officer under delegated authority
Version	5.0
Status	Approved
Effective date	01 September 2026
Last review	September 2026
Next scheduled review	September 2027
Review frequency	At least annually and after a serious data breach or cyber incident, significant audit finding, material system or service change, or relevant legal or regulatory change
Document classification	Public. Suitable for publication on the Future Projects and Future Education websites.

Contents

Part A. Organisation-wide policy
1. Policy statement
2. Purpose, scope and objectives
3. Organisational context and information
4. Legal and standards framework
5. Definitions and information classification
6. Governance, accountability and responsibilities
7. Data protection principles and lawful processing
8. Transparency, privacy information and consent
9. Individual rights and data protection complaints
10. Records management
11. Information security
12. Bring Your Own Device and remote working
13. Data sharing, processors and international transfers
14. Privacy by design and Data Protection Impact Assessments
15. Personal data breaches and cyber incidents
16. Artificial intelligence and automated tools
17. Training, monitoring, audit and assurance
18. Equality, safeguarding and confidentiality
19. Review, approval and linked policies
Appendix A. Information classification and handling matrix
Appendix B. Privacy screening and DPIA process
Appendix C. Personal data breach action card
Appendix D. Records retention schedule
Appendix E. BYOD user conditions

Part B. Future Education supplement

B1. Status and application

B2. Why additional school arrangements are needed
B3. Quick rules for staff
B4. School roles and accountability
B5. Students, parents/carers and accessible privacy
B6. Safeguarding and information sharing
B7. Photos, video, audio and CCTV
B8. Filtering and monitoring
B9. EdTech and artificial intelligence
B10. Future Education retention schedule
B1. Staff action cards

Part C. Privacy information and notices
C1. General Future Projects privacy statement
C2. Child-friendly Future Education privacy summary
C3. Future Education privacy notice – Students, parents and carers
C4. Future Education privacy notice – workforce
C5. Future Education privacy notice – governors and governance roles
C6. Review, accessibility and changes

How to use this document
Part A is the main Future Projects policy and applies across the charity, including Future Education, because The NR5 Project, trading as Future Projects, is the legal entity and is normally the data controller.

Part B adds the school-specific arrangements. Part C contains the school privacy notices. Staff should use the quick rules and action cards in Part B for day-to-day decisions.

Part A. Organisation-wide policy

This part applies across all Future Projects services. Future Education is included because it is operated by The NR5 Project, trading as Future Projects, rather than by a separate legal entity. Part B adds the school-specific controls needed for education, safeguarding, SEND and online safety.

1. Policy statement

Future Projects is committed to respecting privacy, protecting the rights and dignity of individuals, and maintaining trustworthy records and secure information systems. The NR5 Project, trading as Future Projects, is the legal entity responsible for the charity's activities, including Future Education. Personal information will therefore be handled under one organisation-wide framework, lawfully, fairly, transparently and only to the extent needed to deliver our charitable, educational, employment, governance and operational responsibilities.

Future Projects is a local charity delivering community support, specialist education through Future Education, community radio through Future Radio, and central charitable functions. Across these services we routinely handle information about children, families, employees, volunteers and adults who may be vulnerable, including health, safeguarding, SEND, financial, housing, education and criminal-offence information. Our controls will therefore be proportionate to the sensitivity of the information, the vulnerability of the people involved and the risks created by the activity.

Information governance is wider than compliance with data protection law. It includes the quality, availability, security, accessibility, retention and lawful use of all records, whether personal or non-personal, digital or paper. Good information governance enables safe services, continuity, accountability, learning and effective partnership working.

Future Projects will provide appropriate people, authority, systems, training and resources to implement this policy. Privacy and security will be considered from the start of new projects and changes, not added after decisions have been made. All suspected personal data breaches and cyber incidents must be reported immediately so that harm can be contained and legal duties met.

The charity will apply a supportive and accountable approach. Genuine mistakes and concerns should be reported promptly and will be used to improve systems. Deliberate misuse, concealment, reckless handling or repeated disregard of this policy may be managed under disciplinary, volunteer, contractual or safeguarding procedures.

2. Purpose, scope and objectives

2.1 Purpose

This is Future Projects' main policy for data protection, information governance and information security. It sets the rules that apply across the whole charity, with additional requirements for services such as Future Education where the information or risks are more sensitive.

2.2 Scope

This policy applies to the whole of Future Projects and to every service, function, premises and activity operated by the charity. This includes Future Education, Future Support, Future Radio, central functions, outreach, events, remote working, partnership delivery and any new or renamed service. It applies to employees, Trustees, Governors, agency workers, contractors, consultants, temporary workers, volunteers and delivery partners whenever they handle, access or can affect Future Projects information.

Volunteers do not receive access to personal records or restricted systems by default. Where a volunteer role genuinely requires access to personal information, that access must be necessary, proportionate, formally authorised, limited to the minimum required and supported by appropriate confidentiality, safeguarding, security and training arrangements.

The policy covers personal and non-personal information in any form, including databases, cloud services, servers, email, Microsoft Teams, documents, photographs, audio and video, paper files, incident books, notebooks, removable media, telephones and information held by processors or partners on our behalf. It applies on-site, during outreach, remote working, travel and business continuity arrangements.

2.3 Objectives

- Comply with applicable data protection, privacy, records, safeguarding, education, employment and charity requirements.
- Protect people from avoidable harm, distress, discrimination, financial loss, identity misuse and loss of confidentiality.
- Maintain accurate, complete, accessible and trustworthy records that support safe and effective services.
- Ensure access is limited to authorised people for legitimate work purposes.
- Apply consistent security controls across systems, devices, premises, suppliers and remote working.
- Provide clear privacy information and practical routes for people to exercise their rights or complain.
- Build privacy, accessibility and security into new services, projects, systems and data-sharing arrangements.
- Identify, contain, assess, record and learn from personal data breaches and cyber incidents.
- Retain information only for as long as it is needed and dispose of it securely.
- Provide proportionate assurance to senior leaders, Trustees, regulators, funders and partners.

3. Organisational context and information

Future Projects processes information for different purposes and with different risk profiles. The examples below are illustrative and do not replace the organisation's information asset register, privacy notices or records of processing activities.

Area	Typical information	Principal systems and records
Future Support	Service-user identity and contact details; support assessments and case notes; housing, welfare, finance, employability, wellbeing, health, safeguarding and referral information; outcomes and consent records.	Baseline Database; Microsoft 365 and SharePoint; secure paper records where necessary; project and partner systems approved for use.
Future Education	Student, parent and carer information; education, attendance, EHCP, behaviour, health, medical, safeguarding, assessment and staff records.	Cloud-based school management systems; approved safeguarding and education systems; Microsoft 365; specialist filtering and monitoring services; secure paper records.
Future Radio	Employee, volunteer, guest, contributor, supporter and partner details; programme, consent, broadcast, event, contact and commercial records.	Microsoft 365; approved broadcast and production systems; secure contact and consent records.
Central functions	Employee and applicant records; payroll, finance, banking, donor, fundraising, supplier, insurance, governance, Trustee, Governor, contract and risk information.	Microsoft 365 and SharePoint; organisation servers; approved finance, payroll and HR systems; secure governance and paper records.

3.1 Categories of information

Information may include ordinary personal data, special-category data and criminal-offence data. Special-category data includes information about health, disability, race or ethnic origin, religion or belief, political opinion, trade-union membership, genetics, biometrics used for identification, sex life and sexual orientation. Criminal-offence data includes allegations, investigations, cautions, convictions, barring information and related security measures.

Future Projects also holds important non-personal records, including contracts, policies, financial records, risk assessments, minutes, intellectual property, system configurations and operational plans. These records may still be confidential or security-sensitive and are protected under the information-classification arrangements in this policy.

3.2 Controller and processor roles

The NR5 Project, trading as Future Projects, is the legal entity that operates the charity's services and is normally the data controller for information collected and used for its own purposes. This includes personal data processed through Future Education: the school is part of Future Projects and is not a separate legal entity or separate controller simply because it operates as a school. Future Education's Governing Body provides school-level oversight, but legal accountability remains with the charity where Future Projects determines why and how the data is processed. In some commissioned, statutory or partnership arrangements the role may differ and Future Projects may act as a joint controller or processor. The controller/processor role, lawful basis, responsibilities, security and incident-reporting routes must be established and documented before processing begins.

3.3 Future Education – specific application

Future Education is an independent specialist school within Future Projects. Because it works with children aged 13–16 with SEND and SEMH needs, school records can contain particularly sensitive education, health, disability, behaviour, safeguarding, family and social-care information. The organisation-wide requirements in this policy therefore apply in full, with additional school safeguards where needed.

The Headteacher is responsible for day-to-day implementation in school. The Future Education Governing Body provides scrutiny and assurance; the Designated Safeguarding Lead controls safeguarding practice and access to child-protection information; the SENCO supports appropriate handling of SEND information; the IT Manager leads technical security; and Laura Knight remains the organisational DPO/DPL for the school as part of Future Projects.

Future Education must also follow current education-specific requirements and guidance, including Keeping Children Safe in Education 2026, the Independent School Standards, current DfE data-protection guidance, the School Attendance (Student Registration) (England) Regulations 2024 where applicable, and DfE filtering and monitoring standards. Privacy information and rights processes must be understandable and accessible to Students, with reasonable adjustments for SEND and communication needs.

Safeguarding information must be shared lawfully and promptly where needed to protect a child. Data protection law must never be treated as a reason to withhold necessary safeguarding information or delay safeguarding action.

4. Legal and standards framework

Future Projects will comply with applicable law and authoritative guidance, including as amended or replaced:

- UK General Data Protection Regulation.
- Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 and subsequent commencement regulations.
- Privacy and Electronic Communications (EC Directive) Regulations 2003 where electronic communications, cookies or direct marketing are used.
- Human Rights Act 1998 and Equality Act 2010.
- Care Act 2014, Children Acts 1989 and 2004, Education Act 1996 and applicable safeguarding and education requirements.
- Education (Independent School Standards) Regulations 2014 and current Department for Education guidance for independent schools.
- Keeping Children Safe in Education 2026 and Working Together to Safeguard Children 2026.

- School Attendance (Student Registration) (England) Regulations 2024 where applicable to school records and attendance.
- Department for Education data-protection-in-schools guidance, including current guidance on privacy notices, records management, EdTech, AI, CCTV/images, cyber security and filtering and monitoring.
- Health and Safety at Work etc. Act 1974, employment, charity, financial, taxation, contractual and limitation requirements relevant to particular records.
- Common-law duties of confidentiality where applicable.
- Information Commissioner's Office guidance and codes, National Cyber Security Centre guidance and the Data Security and Protection Toolkit where applicable to services and contracts.

Future Projects is not generally a public authority for the purposes of the Freedom of Information Act 2000. It will nevertheless respond appropriately to lawful information requests, contractual transparency duties and requests from statutory bodies, while protecting personal information and legal privilege.

Where the law, a statutory requirement or a contract imposes a higher standard than this policy, the higher standard will be followed. Where requirements appear to conflict, the Data Protection Officer will obtain appropriate advice and record the decision.

5. Definitions and information classification

Term	Meaning
Personal data	Information relating to an identified or identifiable living person, including information that can identify someone when combined with other information.
Special-category data	Personal data requiring additional protection under Article 9 of the UK GDPR, including health, disability, ethnicity, religion, sexual orientation and certain biometric information.
Criminal-offence data	Information about criminal allegations, proceedings, convictions, cautions, barring, offences or related security measures.
Processing	Any operation involving information, including collecting, recording, organising, viewing, sharing, changing, storing, analysing, archiving or deleting it.
Data subject	The living person to whom personal data relates.
Controller	The organisation that decides why and how personal data is processed.
Processor	An organisation that processes personal data on documented instructions from a controller.
Record	Information created, received and maintained as evidence of an activity, decision, obligation or transaction.
Information asset	A defined body of information, system, service or record set that has value and requires an owner and controls.
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
DPIA	A Data Protection Impact Assessment: a structured assessment of privacy risks and controls for processing likely to result in high risk, or where Future Projects decides that formal assessment is prudent.
BYOD	Bring Your Own Device: authorised use of a personally owned device to access Future Projects systems or information.

5.1 Information classification

All information must be handled according to its sensitivity and the consequences of loss, alteration or inappropriate disclosure. The classifications are Public, Internal, Confidential and Restricted. The detailed handling matrix is at Appendix A. When uncertain, staff must use the higher classification and seek advice.

6. Governance, accountability and responsibilities

6.1 Board of Trustees

The Board of Trustees has ultimate oversight of information governance and data protection. It will receive proportionate assurance on significant risks, breaches, complaints, audit findings and improvement actions and will ensure that sufficient governance and resources are available.

6.2 Chief Executive Officer

The Chief Executive Officer is executively accountable for this policy and will:

- ensure appropriate organisational arrangements and resources are in place;
- support the independence and authority of the Data Protection Officer;
- be informed promptly of significant breaches, complaints, regulatory issues and high residual risks;
- approve decisions to proceed with significant residual privacy risk after advice from the Data Protection Officer;
- authorise external legal, forensic, cyber or specialist support where required;
- ensure serious matters are escalated to Trustees and external bodies where appropriate.

6.3 Data Protection Officer

Laura Knight, Finance & Business Support Officer, is Future Projects' organisational Data Protection Officer (DPO) and Data Protection Lead (DPL), covering all services including Future Education. The DPO may be contacted at l.knight@futureprojects.org.uk or at The Baseline Centre, 65-67 Knowland Grove, Norwich, NR5 8YD.

The DPO will act independently when advising on data protection compliance and has direct access to the Chief Executive Officer and, where necessary, the Board of Trustees. Any other duties must not create a conflict of interest with the DPO role. Where a matter concerns a processing decision in which the DPO has had another operational role, the conflict will be declared and independent senior or external advice obtained where appropriate. The DPO will:

- advise the charity, staff and managers on data protection obligations and good practice;
- monitor compliance, training, audits, policies and improvement actions;
- maintain or oversee the information asset register, records of processing, DPIA register, breach register, rights-request log and data protection complaints log;
- advise on lawful bases, special-category and criminal-offence processing, privacy notices, data sharing, contracts and international transfers;
- advise whether a DPIA is required and review completed assessments;
- coordinate individual-rights requests and data protection complaints;
- assess personal data breaches and coordinate notifications to the Information Commissioner's Office and affected individuals where required;
- provide an annual assurance report and prompt reports on significant matters;
- act as the primary contact for the Information Commissioner's Office and cooperate with regulators.

6.4 IT Manager

The IT Manager is the technical security lead and will:

- maintain proportionate technical security standards for accounts, devices, networks, servers, cloud services, backups and monitoring;
- administer or oversee approved-device controls, Microsoft Company Portal, multifactor authentication, access restrictions, malware protection, patching and account security;
- approve devices and technical systems before they access organisational information;

- implement joiner, mover and leaver access changes promptly, including immediate removal when a person leaves;
- assess and contain cyber incidents with the DPO and activate business continuity arrangements where necessary;
- maintain weekly off-site backups of critical files and systems and arrange proportionate restoration testing;
- provide security advice for procurement, projects, DPIAs and supplier reviews;
- ensure equipment is securely configured, repaired, reused and disposed of.

6.5 Heads of Service, managers and information asset owners

Managers are responsible for information handled within their services and will:

- identify information assets, purposes, users, risks, retention periods and suppliers;
- ensure staff access is necessary, authorised and reviewed;
- ensure records are accurate, timely, complete, accessible and stored in approved locations;
- complete privacy screening before new or materially changed processing begins;
- ensure privacy information, consent arrangements and data-sharing agreements are in place where needed;
- report and respond to breaches, complaints, rights requests and audit findings;
- ensure retention and secure disposal requirements are followed;
- provide role-specific instruction, supervision and assurance.

6.6 Employees, Trustees, Governors, agency workers and contractors

Everyone covered by this policy must:

- handle information only for authorised work purposes and in accordance with instructions;
- use individual accounts and approved systems and devices;
- protect passwords, multifactor authentication prompts, devices, papers and conversations;
- check recipients, attachments, sharing permissions and identity before disclosure;
- create accurate records and store them in the appropriate official system;
- not access information out of curiosity or use it for personal benefit;
- report suspected breaches, cyber incidents, loss, inappropriate access and rights requests immediately;
- complete required training and cooperate with reviews and investigations;
- maintain confidentiality during and after their relationship with Future Projects.

6.7 Processors, partners and suppliers

Processors and partners must comply with contractual confidentiality, security, data protection, retention, assistance and breach-notification requirements. They must not use Future Projects information for their own purposes, appoint unauthorised sub-processors or transfer information unlawfully. Future Projects may seek assurance, audit evidence or corrective action according to risk.

7. Data protection principles and lawful processing

7.1 Data protection principles

Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not reused incompatibly;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary;
- protected by appropriate technical and organisational measures;
- handled in a way that enables Future Projects to demonstrate compliance.

7.2 Lawful basis

A valid lawful basis must be identified and documented before personal data is collected or used. Depending on the activity, this may be consent, contract, legal obligation, vital interests, public task or legitimate interests. Consent must not be used merely because it appears convenient, particularly where there is an imbalance of power or a service cannot realistically be refused.

Where legitimate interests are relied upon, the purpose, necessity and impact on individuals must be considered and documented unless the processing falls within a recognised legitimate interest that does not require the full balancing assessment. Public task will only be used where the task has a clear basis in law.

7.3 Special-category and criminal-offence data

Special-category data requires both an Article 6 lawful basis and an Article 9 condition. Criminal-offence data must be processed under official authority or a condition in UK law. Where required by the Data Protection Act 2018, Future Projects will maintain an appropriate policy document explaining the condition, safeguards and retention arrangements.

Access to health, safeguarding, equality, criminal justice, DBS and similar information must be limited to roles that need it. Information must not be recorded simply because it is interesting or might be useful later.

7.4 Data minimisation, accuracy and purpose changes

Forms, systems, reports and data extracts must collect and display only information needed for the stated purpose. Staff must correct inaccuracies promptly, record the source of disputed information where appropriate and distinguish fact, professional judgement and information provided by others.

Before information is reused for a materially different purpose, the manager and DPO must assess compatibility, lawful basis, fairness, transparency and impact. New privacy information or consent may be required. Any permitted reuse must remain necessary and proportionate.

8. Transparency, privacy information and consent

8.1 Privacy information

Future Projects will provide clear privacy information when personal data is collected and, where information is obtained from another source, within the legally required period unless an exemption applies. Privacy notices will explain the controller, purposes, lawful bases, categories, recipients, retention, transfers, rights, complaint routes and any material automated decision-making.

Privacy information will be concise, accessible and written in Plain English. Layered, Easy Read, large-print, audio, child-friendly or other formats will be used where reasonable. Service-specific notices may sit beneath the organisation's overarching privacy notice.

8.2 Fair collection

People should not be misled about why information is requested, whether it is mandatory, what will happen if it is not provided, or who will receive it. Staff must use approved forms and notices and must not create informal data collections without manager and DPO awareness.

8.3 Consent

Where consent is the lawful basis, it must be freely given, specific, informed, unambiguous and recorded. Requests for consent must be separate from unrelated terms and must explain how consent can be withdrawn. Withdrawal must be as easy as giving consent and will not affect processing already carried out lawfully.

The ability of a child or adult to understand and give valid consent must be considered. Where a person lacks capacity for a specific decision, staff must follow the Mental Capacity Act 2005, safeguarding requirements and the appropriate lawful basis rather than treating another person's agreement as automatic consent.

8.4 Images, audio, broadcast and publicity

Photographs, recordings, broadcasts, case studies and publicity involving identifiable people must use an appropriate lawful basis and approved information or consent arrangements. Particular care is required for children, service users, people at risk and material that may reveal health, safeguarding or other special-category information.

8.5 Electronic communications and online services

Electronic marketing, fundraising communications, cookies and similar technologies will comply with data protection law and the Privacy and Electronic Communications Regulations. People's preferences and objections must be respected. Online services likely to be used by children must take children's needs and best interests into account by design.

9. Individual rights and data protection complaints

9.1 Individual rights

Depending on the circumstances, people may have rights to be informed, access their information, rectify inaccuracies, erase information, restrict processing, receive portable information, object to processing and obtain safeguards concerning automated decision-making. Rights may be limited by lawful exemptions and do not override safeguarding, legal, regulatory or third-party rights automatically.

9.2 Recognising and forwarding requests

A request does not need to quote legislation or use a particular form and may be made verbally, in writing, by email or through another member of staff. Any request concerning personal information must be forwarded to the DPO immediately. Staff must preserve relevant records and must not delete, alter or withhold information because a request has been made.

9.3 Response process

The DPO will verify identity proportionately, clarify the scope where reasonably necessary and coordinate a reasonable and proportionate search. Requests will be answered without undue delay and normally within one calendar month. Where a request is complex or numerous, the period may be extended by up to two further months and the person will be informed within the initial month. Information will normally be provided free of charge and in an accessible form.

Information about other people, safeguarding, legal privilege, confidential references and other exempt material will be considered carefully. Any refusal or restriction will be documented and explained, including the right to complain to the Information Commissioner's Office.

9.4 Data protection complaints

Anyone may complain about how Future Projects has handled personal information by contacting the DPO at l.knight@futureprojects.org.uk or by writing to the Data Protection Officer, Future Projects, The Baseline Centre, 65-67 Knowland Grove, Norwich, NR5 8YD. Reasonable adjustments and alternative formats will be provided where needed.

The DPO will ensure that the complaint is recorded and acknowledged within 30 days. Appropriate enquiries will be made without undue delay, the complainant will be kept informed where a response is not immediate, and the outcome and any action will be communicated without undue delay. Complaints will be handled fairly and, where appropriate, by someone not directly involved in the matter.

People will be informed of their right to complain to the Information Commissioner's Office. No person will be disadvantaged for raising a genuine data protection concern or exercising a right.

9.5 Children, Students and parental requests

A child's personal data belongs to the child for data-protection purposes. A Student who can understand the nature and implications of a data-rights request may exercise the right themselves or authorise another person to act for them. Competence will be considered case by case, taking account of age, maturity, understanding, communication needs, SEND and the sensitivity and consequences of disclosure.

Where a Student is not able to exercise the right themselves, a person with parental responsibility may normally act on the Student's behalf where this is appropriate and in the Student's best interests. Where the Student is competent, a parent or carer will normally need the Student's authority to make a subject access request on their behalf.

As an independent school, Future Education does not rely on the separate parental educational-record access regime that applies to maintained schools and non-maintained special schools. Requests for personal data are handled under data-protection law, alongside the school's normal arrangements for reports and communication with parents and carers.

10. Records management

10.1 Record lifecycle

Records must be managed from creation or receipt through active use, storage, review, archiving and secure disposal. The value, sensitivity, legal requirements, operational need and rights of individuals must be considered at each stage.

10.2 Creation and quality

Records must be clear, accurate, contemporaneous, relevant and sufficiently complete to explain the activity, decision and outcome. Staff must use approved templates and systems, date entries, identify the author, distinguish fact from opinion and correct errors transparently rather than obscuring the audit trail.

10.3 Information asset register and records of processing

The DPO will maintain or oversee proportionate records of information assets and processing activities. Managers must provide current information about purposes, categories, lawful bases, sources, recipients, systems, processors, locations, access, retention, security and transfers. Material changes must be reported before implementation.

10.4 Approved storage and filing

Digital records must be stored in approved organisational systems, servers, SharePoint locations or specialist systems with appropriate permissions and backups. Personal data must not be kept in personal email, personal cloud storage, local folders, unapproved applications or removable media unless specifically authorised and protected.

Paper records must be kept in lockable cabinets or secure rooms. Keys and access must be limited to authorised people. Paper files must not be taken home. Where paperwork is exceptionally needed during outreach, it must remain under the authorised worker's control, be returned promptly, scanned to the appropriate secure digital record where required and placed in confidential waste.

10.5 Email, Teams and working records

Email and Teams messages are not substitutes for official case, Student, HR, finance, governance or incident records. Information that evidences a decision, consent, assessment, action or outcome must be transferred to the appropriate official record. Duplicate and transient copies should then be deleted when no longer needed.

10.6 Naming, version control and access

Records must use meaningful file names, dates and version numbers where appropriate. Final or approved documents must be identifiable and protected from accidental alteration. Access must be role-based and reviewed when responsibilities change. Restricted information should not be copied into general shared areas merely for convenience.

10.7 Retention and review

Information will be retained according to Appendix D and any applicable service, school, safeguarding, contractual or statutory schedule. Retention periods are measured from the relevant trigger, such as case closure, the end of employment or expiry of a contract. Managers must review records and dispose of them when the period ends unless a documented reason requires continued retention.

Destruction must be suspended where information may be relevant to a current or anticipated safeguarding matter, complaint, rights request, audit, investigation, insurance claim, litigation, regulatory enquiry or legal hold. The reason and review date must be recorded.

10.8 Secure disposal and archiving

Paper containing confidential or restricted information must be placed in designated confidential-waste bins for collection by an approved provider or securely shredded where authorised. Electronic records and equipment must be securely erased or destroyed under IT Manager oversight. Ordinary deletion is not sufficient where information remains recoverable or on unmanaged media.

Backups are for resilience and recovery, not an alternative archive. Information deleted from live systems will expire from backups through the controlled backup cycle unless a legal or operational hold applies. Archived records must remain indexed, protected and retrievable for authorised purposes.

11. Information security

11.1 Risk-based security

Future Projects will use proportionate technical and organisational measures to protect confidentiality, integrity and availability. Controls will reflect information classification, volume, vulnerability of people, system exposure, operational dependency and credible threats. Security requirements will be reviewed when systems, risks or services change.

11.2 Identity, authentication and access

- Each user must have an individual account. Shared accounts are prohibited unless technically unavoidable, formally approved and controlled.
- Multifactor authentication is required for Microsoft 365 and other systems where supported and appropriate.
- Access must follow least-privilege and need-to-know principles and be approved by the relevant manager or system owner.
- Organisational sign-in controls restrict access to users within the United Kingdom and to company-issued or IT-approved devices, subject to authorised exceptions managed by the IT Manager.
- Access will be removed immediately when a person leaves and adjusted promptly when roles change.
- Privileged and administrative access will be limited, separately controlled where practicable and reviewed according to risk.
- Unexpected multifactor prompts, unusual sign-ins or suspected credential compromise must be reported immediately.

11.3 Passwords and account security

Passwords and passphrases must be strong, unique and not shared or reused for personal services. Users must not approve unexpected multifactor prompts or disclose authentication codes. Passwords must be changed immediately when compromise is suspected and in accordance with system or IT instructions.

11.4 Devices and endpoint protection

Organisation-issued devices will be configured and managed by or under the oversight of the IT Manager. Antivirus, malware protection, firewall, security updates, patching and screen-lock controls will be applied proportionately. Specialist filtering and monitoring controls are maintained at Future Education to protect Students, staff and systems and to manage access to inappropriate or harmful online content.

Portable devices authorised to store personal data locally must use appropriate encryption. Where full-device encryption is not enabled, confidential and restricted information must be accessed through approved managed systems and must not be stored locally. Removable media may only be used where authorised, encrypted and recorded.

11.5 Servers, networks and backups

Future Projects maintains its own servers and approved cloud services. Critical files and systems are backed up weekly to an off-site location. Backup access will be separated from routine user access where practicable, retention will follow a defined cycle and restoration will be tested proportionately, including after material system changes. Backups must be protected from unauthorised alteration, ransomware and loss.

Network, wireless and server configurations will be managed by the IT Manager or approved specialists. Unauthorised devices, software, services, remote-access tools or changes must not be introduced.

11.6 Email, Teams and secure transfer

Future Projects uses Microsoft 365, including available encryption and secure-sharing options. Staff must verify recipients, addresses, attachments, permissions and sensitivity before sending. Sensitive information should use the minimum necessary content, approved secure links or encryption and an appropriate separate communication of passwords where required.

Personal email, consumer file-sharing services, unapproved cloud storage and consumer messaging applications must not be used for personal, confidential or restricted work information. Large distribution lists must use appropriate permissions or blind-copy controls to prevent unnecessary disclosure.

11.7 Physical and environmental security

Confidential work areas, filing, servers and equipment must be protected from unauthorised access. Staff must follow clear-desk and clear-screen practice where information could be viewed by others, lock screens when unattended, manage visitors and avoid confidential discussions where they can be overheard.

11.8 Logging, monitoring and investigation

Future Projects may log and monitor access, security events, network activity, email, devices and system use where lawful, proportionate and transparent. Monitoring is used to protect people, systems and information, meet safeguarding and regulatory duties and investigate suspected misuse. Monitoring records are restricted and retained according to need.

11.9 Equipment repair, reuse and disposal

Devices must be returned to the IT Manager for repair, reassignment or disposal. Storage media will be securely erased, destroyed or retained under controlled conditions before equipment leaves organisational control. Staff must not sell, donate, discard or privately repair work devices.

11.10 Future Education filtering and monitoring

Filtering and monitoring at Future Education are safeguarding controls as well as information-governance activities. The Governing Body/proprietor has strategic responsibility for assurance. The school must identify a responsible senior leader and governor; the DSL leads safeguarding use of alerts and reports; and the IT Manager or approved IT provider maintains the technical controls.

The provision must be reviewed at least once every academic year by senior leadership with the DSL and IT support, involving the responsible governor. The review and actions must be recorded and must take account of the school's Student profile, including age, SEND, SEMH needs, vulnerability, off-site use and the limitations of filtering and monitoring in relation to dynamic, personalised and AI-generated content.

Technical monitoring must be transparent, proportionate and covered by privacy information and a DPIA where required. As a minimum, the monitoring plan should provide weekly reports highlighting incidents and immediate reporting of high-risk incidents. Safeguarding alerts and evidence must be handled under school safeguarding procedures and retained in the appropriate safeguarding or incident record where necessary.

12. Bring Your Own Device and remote working

12.1 Permitted BYOD use

Personal phones may be authorised to access Outlook and Microsoft Teams only where the device is approved by the IT Manager and enrolled in Microsoft Company Portal. Company Portal enforces required security controls and

enables corporate access to be blocked and corporate information to be removed if the device is lost, stolen, non-compliant or no longer authorised.

Personal laptops, desktop computers and tablets are not permitted by default. Any exception requires prior written IT Manager approval, a documented risk assessment and controls equivalent to those required for an organisation-issued device.

12.2 Conditions of access

- The device must remain within supported software versions, use a secure screen lock and not be rooted, jailbroken or shared with another person.
- The user must allow Company Portal and organisational access controls to enforce security requirements and remove corporate access or work data where necessary.
- Personal devices may access approved company systems remotely but must not store, download, copy, photograph, screen-record or back up personal, confidential or restricted information to personal storage or applications.
- Personal devices must not be used to access service-user case systems, Student systems, HR, payroll, finance, safeguarding or other restricted systems unless a separate written authorisation explicitly permits it.
- Work information must not be forwarded to personal email, messaging, cloud storage or other personal accounts.
- Loss, theft, suspected compromise, unexpected authentication prompts or loss of control of the device must be reported immediately to the IT Manager and DPO.
- Access may be restricted or withdrawn at any time according to risk, system change, employment status or non-compliance.

12.3 Organisational and personal privacy

Future Projects owns and controls corporate accounts and data accessed through BYOD. The organisation may manage the work profile, check device compliance, revoke sessions and remove corporate information. It will not intentionally access personal photographs, messages or content outside the managed work environment, but users should understand the capabilities and implications of device management before enrolling.

12.4 Remote working

Remote work must protect privacy to the same standard as office work. Staff must use approved devices and systems, prevent family or others from viewing information, avoid confidential calls in public, use trusted network connections, lock screens when unattended and store no paper records at home. Printing personal information at home is prohibited unless specifically authorised for an exceptional reason and secure return or destruction arrangements are agreed.

Detailed BYOD conditions are set out at Appendix E. Use of a personal device is optional unless expressly agreed for the role; an organisation-issued alternative will be considered according to operational need and resources.

13. Data sharing, processors and international transfers

13.1 Sharing decisions

Personal data may only be shared where there is a clear purpose, lawful basis and authority. Staff must confirm the recipient's identity, share the minimum necessary information, use an approved secure method and record significant disclosures. Consent is not always required, particularly where sharing is necessary for safeguarding, vital interests or a legal duty, but the decision must be lawful and proportionate.

13.2 Data-sharing arrangements

Regular, systematic or sensitive sharing should be supported by a data-sharing agreement, information-sharing protocol or contract. The document should cover purpose, roles, lawful basis, information, security, accuracy, retention, rights, complaints, breaches, review and exit arrangements. Emergency sharing may proceed where lawful and necessary, with the rationale recorded afterwards.

13.3 Processors and cloud services

Before appointing a processor, Future Projects will assess capability, security, location, sub-processors, resilience, deletion, incident history and assurance according to risk. Contracts must contain the required data-processing terms, including documented instructions, confidentiality, security, assistance with rights and breaches, deletion or return, audit and control of sub-processors.

No employee may introduce or upload organisational information to an unapproved cloud service, application, trial account or software-as-a-service product. Procurement and renewal decisions involving personal information must include the DPO and IT Manager at an appropriate stage.

13.4 International transfers

Personal data will not be transferred or made remotely accessible outside the United Kingdom unless an appropriate legal transfer mechanism and safeguards are in place. This may include adequacy regulations, an approved transfer instrument and a documented assessment of protection and risk. Supplier statements alone are not sufficient where formal safeguards are required.

14. Privacy by design and Data Protection Impact Assessments

14.1 Privacy by design and default

Privacy, accessibility and security must be considered at the earliest stage of a new project, service, system, form, partnership, data-sharing arrangement, monitoring activity or material change. Default settings must limit collection, access, sharing and retention to what is necessary. Managers must not sign contracts, launch processing or collect live personal data before required review and approval are complete.

14.2 Initial privacy screening

The manager leading the change will complete an initial privacy screening and provide it to the DPO. Screening is required where the activity creates a new purpose or data set, uses a new supplier or technology, links data sources, changes access or sharing, involves children or vulnerable people, introduces monitoring, uses artificial intelligence or materially changes risk.

14.3 When a DPIA is required

A DPIA must be completed where processing is likely to result in high risk to people. Indicators include:

- large-scale or systematic processing of special-category or criminal-offence data;
- systematic monitoring, tracking, profiling or surveillance;
- innovative technology, artificial intelligence or novel combinations of technology and sensitive data;
- matching or combining data sets in ways people may not reasonably expect;
- processing that could prevent people accessing a service, benefit or opportunity;
- processing involving children, people at risk or others who may be less able to exercise their rights;
- biometric identification, location tracking or automated decisions with legal or similarly significant effects;
- any change where a breach, error or misuse could plausibly cause serious harm.

The DPO may advise that a DPIA should be completed in other circumstances as good practice. Where screening concludes that a DPIA is not required, the reasoning must be recorded.

14.4 DPIA responsibilities and approval

The service or project manager owns the DPIA and describes the processing, necessity, proportionality, consultation, risks and controls. The IT Manager provides technical and security information. Relevant staff, partners and people affected will be consulted where proportionate and safe. The DPO advises on legal compliance, adequacy of controls and residual risk and records the assessment on the DPIA register.

The responsible manager remains accountable for the processing and may proceed only when required controls are in place, having considered the DPO's advice. Where significant residual risk remains, the CEO must decide whether to stop or redesign the activity and whether prior consultation with the Information Commissioner's Office is required. The decision and rationale must be documented.

14.5 Review

DPIAs are living documents. They must be reviewed before material changes and after incidents, complaints, audit findings or evidence that assumptions or controls are no longer valid. Appendix B sets out the screening and assessment process.

15. Personal data breaches and cyber incidents

15.1 Immediate reporting

All suspected or confirmed personal data breaches must be reported immediately to the DPO. Cyber-related incidents must also be reported immediately to the IT Manager. Staff must not wait until they are certain or until all facts are known. Outside normal working hours, urgent threats must be escalated through the restricted emergency contact arrangements in the Business Continuity and EPRR Policy and Plan.

15.2 Examples

- misdirected email, post, Teams message or attachment;
- loss or theft of a device, paper record, notebook or storage media;
- unauthorised access, excessive permissions or information viewed out of curiosity;
- phishing, credential theft, malware, ransomware or business email compromise;
- accidental deletion, corruption, alteration or loss of availability;
- information disclosed verbally, displayed or published to the wrong person;
- paper records placed in ordinary waste or left unsecured;
- a supplier or partner incident affecting Future Projects information.

15.3 Immediate action

Staff should stop the activity where safe, prevent further disclosure, preserve evidence and follow IT or manager instructions. They must not delete evidence, wipe or reset devices, communicate with an attacker, contact affected people, make public statements or attempt an unauthorised investigation. Affected devices may be disconnected if safe and instructed.

15.4 Assessment and recording

The DPO and IT Manager will coordinate containment and assess what happened, the information and people affected, sensitivity, volume, accessibility, safeguards, likelihood of misuse, actual and potential consequences and remedial action. Relevant managers, Designated Safeguarding Leads, the CEO, insurers, suppliers or specialists will be involved according to risk.

Every suspected or confirmed personal data breach, including low-risk incidents and false alarms, will be recorded in the breach register with the facts, effects, assessment, decision, action and learning. A related entry will be made under the Incident Reporting and Management Policy where appropriate, without unnecessarily duplicating sensitive detail.

15.5 External notification

Where a breach is likely to result in a risk to people's rights and freedoms, the DPO will coordinate notification to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of Future Projects becoming aware of it. An initial notification may be made where facts are incomplete and supplemented as the investigation develops. The CEO will be informed immediately of any significant or potentially notifiable breach.

Where the breach is likely to result in high risk, affected people will be informed without undue delay in clear and practical language unless a lawful exception applies. Decisions not to notify the ICO or individuals will be documented. Commissioners, funders, safeguarding authorities, police, insurers, banks, professional bodies or other organisations will be informed where required by law, contract or risk.

15.6 Suppliers and recovery

Processors and partners must report breaches affecting Future Projects information without undue delay and provide information and assistance needed to meet legal deadlines. Recovery will follow the Business Continuity and

EPRR Policy and Plan, including containment, secure restoration, data reconciliation, communication and post-incident review. Appendix C provides the immediate action card.

16. Artificial intelligence and automated tools

16.1 Prohibited use

Personal, confidential, commercially sensitive, safeguarding, Student, service-user, employee, donor or partner information must not be entered into public, consumer or otherwise unapproved artificial-intelligence tools. Staff must not use AI to bypass approved systems, make covert recordings, summarise restricted records in personal accounts or train external tools on Future Projects information.

16.2 Approval and safeguards

Any organisational AI use involving personal information requires prior approval from the relevant manager, DPO and IT Manager, initial privacy screening and a DPIA where required. The assessment must consider supplier terms, training use, security, location, retention, transparency, accuracy, bias, explainability, intellectual property, human oversight and the impact on children or vulnerable people.

16.3 Human responsibility

AI outputs must be checked by a competent person before use. AI must not make a solely automated decision with legal or similarly significant effects unless the processing is lawful, necessary, transparent and specifically approved with required safeguards. Responsibility for decisions, records and communications remains with Future Projects and the authorised staff member.

16.4 Future Education and learner-facing AI

Before an AI or EdTech tool is used with Students, Student data or school records, Future Education must involve the DPO and IT Manager and, where safeguarding may be affected, the DSL. The school must understand age restrictions, the supplier's controller/processor role, data location, retention, sub-processors, whether prompts or files are used to train or improve the model, content moderation, monitoring, audit trails and deletion arrangements.

Personal, safeguarding, Student, parent/carer or staff information must not be entered into public or otherwise unapproved AI tools. Approved AI outputs must be checked for accuracy, bias, suitability and safeguarding risk. The effect on Students with SEND or SEMH needs must be considered, and material product changes or new AI features must trigger proportionate re-review of the DPIA, privacy information and safeguards.

17. Training, monitoring, audit and assurance

17.1 Training and awareness

Employees will receive data protection, information security and breach-reporting training during induction and at least annually. Trustees and Governors will receive proportionate training. Volunteers will receive confidentiality, safe-information-handling and incident-reporting awareness, with additional training where an authorised role involves access to personal information.

Enhanced role-specific training will be provided for managers, the DPO, IT staff, Designated Safeguarding Leads, system administrators and people handling special-category, criminal-offence, Student, HR or high-volume information. Training completion will be recorded, monitored and escalated where overdue.

17.2 Monitoring and review

The DPO, IT Manager and managers will use proportionate checks to confirm that the policy is operating in practice. These may include access reviews, record sampling, retention checks, supplier assurance, security monitoring, restoration tests, DPIA reviews, rights-request sampling and follow-up of incidents and audit actions.

17.3 Assurance measures

Assurance reporting may include:

- completion of mandatory and role-specific training;
- number, type, severity and timeliness of breach reports;
- rights requests and data protection complaints completed within required timescales;
- DPIAs and privacy screenings completed before go-live;
- access reviews, leaver removals and device compliance;
- retention reviews and secure disposal completed;
- backup and restoration testing outcomes;
- supplier and data-sharing assurance;
- audit findings and overdue corrective actions.

The DPO will provide an annual report to the CEO and proportionate assurance to Trustees. Significant gaps will be escalated promptly and may be entered in the corporate risk register or business continuity work programme.

17.4 Non-compliance

Failure to follow this policy may result in removal of access, additional training, management action, disciplinary proceedings, termination of a volunteer or contractor relationship, reporting to a regulator or professional body, or legal action. Response will be fair and proportionate and will consider intent, harm, reporting, cooperation and system factors.

18. Equality, safeguarding and confidentiality

18.1 Equality and accessibility

Information governance arrangements must not create avoidable barriers or discrimination. Privacy information, rights processes and complaints routes will be accessible, and reasonable adjustments will be made. Equality information will be restricted and used only for lawful purposes, with anonymised or aggregated reporting wherever possible.

18.2 Safeguarding and information sharing

Safeguarding and protection of life may require information to be shared without consent. Staff must follow the relevant safeguarding policy, involve a Designated Safeguarding Lead and share the minimum necessary with an appropriate person or authority. Confidentiality must not be promised where disclosure may be needed to protect a child or adult at risk.

18.3 Confidentiality

Confidentiality applies to verbal, written, visual and digital information and continues after employment, volunteering, office or contract ends. Information may be shared internally only with those who need it. Professional curiosity must never become unauthorised access. Concerns about improper access or disclosure must be reported immediately.

19. Review, approval and linked policies

19.1 Review and approval

The DPO will review this policy at least annually. An earlier review will take place after a serious personal data breach or cyber incident, significant audit finding, material change to systems, services or processing, change in law or ICO guidance, or evidence that controls are ineffective. Changes will be approved by the Chief Executive Officer under delegated authority and communicated to relevant people.

19.2 Linked organisational policies and procedures

- Business Continuity and Emergency Preparedness, Resilience and Response Policy and Plan.
- Incident Reporting and Management Policy.
- Health and Safety Policy and Lone Working Policy.
- Safeguarding Adults Policy, Safeguarding Children Policy and Future Education safeguarding procedures.

- Future Education Data Protection & Information Governance: School-specific arrangements and records retention schedule.
- Compliments and Complaints Policy and Future Education complaints procedure.
- Equality and Diversity Policy.
- Social Media and Professional Boundaries Policy, Future Education Online Safety Policy and Acceptable Use arrangements.
- DBS, criminal records and safer-recruitment policies and procedures.
- Anti-Fraud, Bribery and Corruption Policy and Conflict of Interest Policy.
- Risk Policy, IT acceptable-use arrangements, privacy notices, data-sharing agreements and service-specific retention schedules.

19.3 External references

- Information Commissioner's Office: data protection principles, individual rights, data protection complaints, data protection by design, DPIAs, security and personal data breach guidance.
- UK Government: Data (Use and Access) Act 2025 and commencement guidance.
- National Cyber Security Centre: device security and Bring Your Own Device guidance.
- DBS Code of Practice and relevant education, safeguarding and records-management guidance.
- Department for Education: Data protection in schools guidance (updated July 2026).
- Department for Education: Keeping Children Safe in Education 2026.
- Department for Education: Filtering and monitoring core standard (updated September 2026).
- Department for Education: Independent school standards guidance (2026).
- Data Security and Protection Toolkit guidance where applicable.

Part B. Future Education supplement

B1. Status and application

Future Education is an independent specialist school within Future Projects. It is not a separate legal entity. The NR5 Project, trading as Future Projects, is therefore normally the data controller for personal information used by the school. Part A applies to the school in full. This supplement adds the arrangements that are different or especially important in an education, SEND, SEMH and safeguarding setting.

It applies to school employees, Governors, agency workers, contractors, consultants, volunteers and others who handle or can access school information, including during trips, outreach, remote working, transport and partnership activity.

One policy suite: There is no separate competing GDPR policy for Future Education. Part A sets the organisation-wide rules; Part B adds the school-specific rules; Part C explains to people how their information is used.

B2. Why additional school arrangements are needed

Future Education works with children and families whose records may contain detailed educational, health, disability, behavioural, safeguarding, family, social-care and criminal-offence information. Students may need information explained or presented differently because of SEND, communication needs or SEMH. The school must therefore be legally compliant and secure while remaining child-centred, accessible and practical.

- Access information only where it is genuinely needed for the person's role.
- Do not treat a Student's diagnosis, disability, behaviour or safeguarding history as general background information that may be shared freely.
- Record facts accurately and distinguish facts, professional judgement and information reported by somebody else.
- Safeguarding comes first. Data protection law supports appropriate information sharing to protect children and must not delay necessary safeguarding action.
- Adapt privacy information, rights requests and explanations so Students can understand and participate as far as possible.

B3. Quick rules for staff

Rule	What this means
Do	Use approved school/charity systems and your own work account.
Do	Check recipients, attachments and sharing permissions before sending.
Do	Keep records accurate, factual, relevant and up to date.
Do	Lock screens and secure paper records whenever you step away.
Do	Share only the information needed for the purpose.
Do	Report suspected data loss, mis-sends, inappropriate access or cyber incidents immediately.
Do	Send data-rights requests and data-protection complaints to the DPO immediately.
Do not	Look at a Student, family or staff record out of curiosity.
Do not	Send school information to personal email or store it in personal cloud accounts.
Do not	Put identifiable Student, parent/carer or staff information into an unapproved AI tool.
Do not	Photograph or record Students on a personal device.
Do not	Promise absolute confidentiality where safeguarding information may need to be shared.
Do not	Delete or alter records because a complaint, request, investigation or incident has arisen.

Rule	What this means
Do not	Create informal forms, spreadsheets, apps or databases collecting personal data without approval.

B4. School roles and accountability

Role	Responsibility
Board of Trustees	Has ultimate oversight of data protection and information governance across Future Projects, including Future Education.
Future Education Governing Body	Provides school-level scrutiny and assurance on significant risks, incidents, complaints, training, filtering/monitoring and improvement actions. It does not replace the legal accountability of the charity as controller.
Headteacher	Responsible for day-to-day implementation in school, ensuring staff understand requirements and that new systems, suppliers and processes are reviewed before use.
Data Protection Officer / Data Protection Lead	Laura Knight is the organisational DPO and DPL for Future Projects and Future Education. She provides independent advice, coordinates rights requests, complaints, DPIAs and breach assessments, and is the main ICO contact.
Designated Safeguarding Lead	Controls safeguarding practice and access to child-protection records and ensures safeguarding information is recorded and shared appropriately.
SENCO	Supports accurate, relevant and proportionate handling of information about Students' additional needs and reasonable adjustments.
IT Manager	Leads technical security, approved devices and systems, access controls, backups, filtering and monitoring technology, incident containment and secure disposal.

B5. Students, parents/carers and accessible privacy

A Student's personal data belongs to the Student for data-protection purposes. A Student who can understand the nature and implications of a data-rights request may exercise the right themselves or authorise another person to act for them. Competence is assessed case by case, taking account of age, maturity, understanding, communication needs, SEND, sensitivity and the consequences of disclosure.

Where a Student is not able to exercise the right themselves, a person with parental responsibility may normally act on the Student's behalf where this is appropriate and in the Student's best interests. Where a Student is competent, a parent/carer will normally need the Student's authority to make a subject access request on their behalf.

As an independent school, Future Education does not rely on the separate parental educational-record access regime that applies to maintained schools and non-maintained special schools. Personal-data requests are handled under data-protection law alongside the school's normal arrangements for reports and communication with parents/carers.

- Use plain English and avoid unnecessary legal language.
- Offer a child-friendly, Easy Read, verbal or other reasonable format where this helps a Student understand.
- Explain sensitive information-sharing calmly and proportionately unless doing so would create a safeguarding or legal risk.
- Do not rely on a parent/carer to explain a Student's data rights where the Student can understand them with appropriate support.

For all staff: A subject access request can be verbal or written and does not need to mention GDPR. If anybody asks for their own personal information, or a parent/carer asks for a Student's personal information, send the request to the DPO immediately and preserve the records in scope.

B6. Safeguarding and information sharing

Information may be shared where necessary and lawful for education, safeguarding, health and welfare, SEND support, statutory duties, commissioning, examinations, law enforcement or other legitimate school purposes. Consent is not always required and should not be sought where another lawful basis is more appropriate.

- Where a child may be at risk, follow the Safeguarding Policy and contact the DSL or deputy without delay.
- Share enough information to make the safeguarding action useful and safe, but no more than is necessary.
- Record what was shared, with whom, why and by whom.
- Use a secure transfer method and verify the recipient.
- Keep child-protection files separately from the main Student record with tightly controlled access.
- When a Student moves school, transfer the child-protection file separately and securely in line with current safeguarding guidance and obtain confirmation of receipt.
- Never promise that safeguarding information will never be shared.

B7. Photos, video, audio and CCTV

Images and recordings of identifiable people are personal data. The lawful basis depends on the purpose. Consent may be appropriate for optional publicity; it should not automatically be used for routine education, administration or safeguarding.

- Check current restrictions before taking, using or publishing an image.
- Do not publish an image of a Student who must not be publicly identified because of safeguarding, court or other restrictions.
- Staff must not use personal devices to take photographs, video or audio of Students. School-provided or formally approved school equipment must be used.
- Store learning, evidence or safeguarding images in the appropriate official system, not personal galleries or consumer messaging apps.
- External photographers and platforms must be covered by appropriate contractual, safeguarding and data-protection arrangements.

CCTV must have a defined purpose, be proportionate, transparent and subject to access controls. Routine footage is normally overwritten after the period stated in the school's current privacy information and retention schedule. Extracted footage needed for an incident, safeguarding matter, complaint, claim or police request follows the longer record period that applies to that matter.

B8. Filtering and monitoring

Filtering and monitoring are safeguarding controls as well as information-governance activities. They must be effective, proportionate, transparent and appropriate to Future Education's Students and risks.

- The Governing Body/proprietor retains strategic responsibility for assurance and the school identifies a responsible senior leader and responsible governor.
- The DSL leads the safeguarding use of alerts and reports; the IT Manager or approved IT provider maintains the technical controls.
- Senior leadership, the DSL and IT support review the provision at least annually, involving the responsible governor. The review and actions are recorded.
- The review considers age, SEND, SEMH, vulnerability, off-site use, personal devices and the limitations of filters with dynamic, personalised and AI-generated content.
- The monitoring plan provides routine reporting and immediate escalation of high-risk incidents. Safeguarding alerts are transferred into the appropriate safeguarding record where needed.
- Monitoring must be explained in privacy information, access to alerts/reports is restricted to authorised people, and a DPIA is completed for new or materially changed monitoring where required.

- Temporary filtering exceptions must be approved and documented by the responsible senior leader, with the DSL assessing any safeguarding implications.

B9. EdTech and artificial intelligence

No app, online platform, AI service or other digital tool may be introduced simply because it is useful or free. The school must understand the data, purpose, supplier role, security, location, retention, deletion, sub-processors and whether information is used for the provider's own purposes or AI training.

- Use only approved AI and EdTech tools for school work.
- Do not enter identifiable Student, parent/carer, staff, safeguarding or other restricted information into a public or unapproved AI tool.
- Involve the DPO and IT Manager before an AI/EdTech tool processes personal information; involve the DSL where Student safeguarding may be affected.
- Complete privacy screening and a DPIA where required before live use.
- Consider age restrictions, accessibility, SEND/SEMH impact, bias, content moderation, safeguarding, human oversight, model-training use and changes to provider terms or features.
- Human staff remain responsible for decisions. AI outputs must be checked for accuracy, suitability and bias before use.
- Do not make solely automated decisions with legal or similarly significant effects unless the use is specifically lawful, transparent and approved with the required safeguards.

B10. Future Education retention schedule

The organisation-wide retention schedule in Appendix D applies unless the school-specific period below is more appropriate. School records must not be kept simply because storage is available. Deletion must stop where a record may be relevant to safeguarding, a data-rights request, complaint, investigation, claim, litigation, police matter, audit or regulatory enquiry.

Legal hold: If a record may be relevant to a safeguarding matter, complaint, subject access request, investigation, claim, litigation, police matter, audit or regulatory enquiry, routine deletion must stop until the DPO or appropriate senior lead confirms it can resume.

Record	Retention / disposal	Notes
Core Student record	Until the Student's 25th birthday At the end: Securely destroy	Adopted school standard. Includes key admissions, identity/contact, curriculum, attainment, progress, behaviour, serious sanctions, significant parent/carer communications, relevant SEND/EHCP material and other information needed to understand the Student's education. On transfer, send what the receiving setting needs securely and retain only what Future Education still needs.
Child protection / safeguarding file	While Future Education is custodian: until the child's 25th birthday. Records known to relate to child sexual abuse: until the child's 75th birthday. At the end: Securely destroy after final review, unless transferred	Keep separately with restricted access. On transfer, send separately from the main Student file, securely and with confirmation of receipt, within KCSIE 2026 timescales. Include a structured summary of current concerns, relevant context and ongoing support needs. The 25/75-year periods are adopted in line with current DfE/IICSA retention guidance.
SEND / EHCP working records	Normally with the core Student record, to the Student's 25th birthday At the end: Securely destroy	There is no separate universal statutory SEND retention period for schools. Keep only information that remains necessary; avoid duplicate copies where the local authority or another body is the long-term record holder.
Admission register entries	6 years from the date the entry is made At the end: Securely destroy	Statutory period under the School Attendance (Student Registration) (England) Regulations 2024.

Record	Retention / disposal	Notes
Attendance register entries and backup copies	Entries: 6 years from the date made. Backup copies: 6 years after the end of the school year to which they relate. At the end: Securely destroy	Statutory period under the 2024 Regulations.
Routine behaviour records	Until no longer needed operationally; significant/serious records form part of the core Student record and are retained to age 25 At the end: Securely destroy	Keep records proportionate. Do not retain minor duplicate records merely because they exist in multiple systems.
Medical, medication and health support records relating to a Student	Material records forming part of the Student's long-term education/welfare record: normally to the Student's 25th birthday. Routine duplicate or short-term administration: delete when no longer needed. At the end: Securely destroy	Health information is special-category data. There is no single statutory school retention period for all medication/health records; retain according to purpose, risk and the wider Student record, and remove duplicate or superseded copies sooner.
Accident / injury records involving Students	At least 3 years where an accident record requirement applies; where material to a Student claim, safeguarding matter or continuing support, retain with the Student record to age 25 or for any longer legal/insurance hold. At the end: Securely destroy	Use the longer period where required by RIDDOR/accident-record rules, limitation periods, insurance, safeguarding or a legal hold. Avoid retaining duplicate copies in multiple systems.
Educational visits: consent, lists and routine administration	10 years from the date of the visit At the end: Securely destroy	Current DfE school data-protection guidance uses 10 years. If an incident occurs, retain the relevant permission slips and incident material with the Student/incident record for the longer applicable period.
Public examination / assessment administration	Follow current awarding-body / JCQ requirements; retain final Student attainment information with the core Student record to age 25 where relevant At the end: Securely destroy when no longer required	Do not retain examination scripts, access-arrangement evidence or working papers longer than required by the relevant rules and any appeal/complaint period.
Student photographs/video for routine internal education or administration	Review at least annually; delete when no longer needed and normally no later than 12 months after the Student leaves unless there is a documented continuing purpose At the end: Securely delete	Safeguarding/evidential images follow the underlying safeguarding or incident record. Published material may require a different documented period.
Publicity / social-media images based on consent	For the stated purpose and period; review when the Student leaves and on withdrawal of consent At the end: Stop new use and delete from controlled locations where required/possible	Withdrawal does not necessarily remove material already lawfully printed, distributed or cached outside the school's control.

Record	Retention / disposal	Notes
CCTV footage	Normally 30 days under the Future Projects organisational schedule At the end: Automatic overwrite / secure deletion	There is no fixed statutory 30-day period. The actual period must be the shortest necessary for the stated purpose and match signage, privacy information and system settings. Extracts linked to an incident, claim, police or safeguarding matter follow the relevant record period.
Filtering, monitoring, access and security logs	Normally 12 months under the Future Projects organisational schedule At the end: Securely delete	The actual period must be documented in the DPIA/privacy information and match system/provider settings. Retain longer only where needed for safeguarding, security, audit or investigation. Material safeguarding evidence should be placed in the safeguarding/incident record.
Visitor and routine sign-in records	12 months At the end: Securely destroy	Longer only where linked to an incident, safeguarding concern or security investigation.
School complaints	6 years after closure At the end: Securely destroy	Safeguarding, legal claims or regulatory matters may require longer. Keep a clear record of outcome and actions.
Subject access / other data-rights requests	6 years after closure At the end: Securely destroy	Keep the request, search/disclosure record, decisions, correspondence and outcome securely.
Personal data breach / cyber incident records	6 years after closure At the end: Securely destroy	Serious incidents may be retained longer for legal, insurance, security or organisational learning.
DPIAs, privacy screening and data-sharing decisions	Duration of the processing plus 6 years At the end: Securely destroy	Keep significant superseded versions and evidence of completed actions.
Staff personnel files	6 years after employment ends At the end: Securely destroy	Central Future Projects HR record. Safeguarding allegations, pension, health or other specialist records may have different periods.
DBS certificate copy	Normally no longer than 6 months after the recruitment decision At the end: Securely destroy	Retain only the permitted record that the check was completed and its outcome/status in the appropriate safer-recruitment/SCR record.
Single Central Record / safer recruitment compliance evidence	Live record only: remove an individual's details once they no longer work at or are engaged by the school At the end: Remove from the SCR promptly when the person leaves	KCSIE 2026 requires leavers to be removed from the SCR. Underlying recruitment/personnel evidence is retained separately under the staff personnel, DBS and safeguarding periods in this schedule; the SCR itself is not a six-year historic archive.
Safeguarding allegation against a member of staff	At least until normal pension/retirement age or 10 years from the allegation, whichever is later At the end: Securely destroy after review	KCSIE 2026: records of allegations are retained at least until normal pension age or 10 years from the allegation, whichever is longer. Details of allegations found to be malicious or false should be removed from personnel records unless the individual consents to retention. Unfounded or unsubstantiated allegations are not treated as malicious/false and remain subject to the retention rule.
Low-level concerns about staff	At least until the person leaves; then review At the end: Securely destroy unless a documented reason requires longer retention	KCSIE 2026 recommends retention at least until the individual leaves. Review for any continuing lawful need, including patterns, disciplinary action, safeguarding risk, complaint or legal issue. If the harm threshold is met, apply the allegation record period.
Governor meeting approved minutes and key governance records	Permanent At the end: Archive	Retain approved versions and key superseded governance records as part of the charity/school governance archive.

Record	Retention / disposal	Notes
Routine governor working papers	6 years after superseded or no longer required At the end: Securely destroy	Longer where they evidence significant safeguarding, contractual, property or legal decisions.

B11. Staff action cards

B11.1 Information has been lost, sent to the wrong person or accessed wrongly

1. Act immediately: if safe, recall the email, remove the sharing link, recover the paper/device or ask the unintended recipient not to use the information and to delete/return it.
2. Report it immediately to the DPO and IT Manager. Tell the Headteacher/DSL as well if a Student or safeguarding matter may be involved.
3. Do not conceal the error, delete evidence or investigate it alone.
4. Record what happened, when, whose information was involved, what you have done and who you have told.
5. Follow the containment instructions you are given.

B11.2 Somebody asks to see their information

6. Treat verbal, written, email and social-media requests seriously. They do not need to say “subject access request” or “GDPR”.
7. Forward the request to the DPO immediately.
8. Preserve relevant records. Do not delete, tidy up, rewrite or withhold material because a request has been made.
9. Continue normal safeguarding and operational work; the DPO will coordinate the legal response.

B11.3 I need to share information to protect a Student

10. Follow the Safeguarding Policy and contact the DSL/deputy without delay.
11. Share with the person or agency that needs the information. Consent is not always required for safeguarding.
12. Share enough to make the information useful and safe, but no more than is necessary.
13. Use a secure method and verify the recipient.
14. Record what was shared, why, with whom and any decision made.

B11.4 I want to introduce a new app, online system, AI tool or supplier

15. Do not start using it with real Student, parent/carer or staff information.
16. Ask the responsible manager/Headteacher to involve the DPO and IT Manager at the outset.
17. Identify what data the tool needs, why, where it is stored, who receives it, retention/deletion, security, international transfers and whether the provider uses it for its own purposes or AI training.
18. Complete privacy screening and a DPIA where required before implementation.
19. Only use the service after approval, contract/data terms and privacy information are in place.

Part C. Privacy information and notices

Part C contains the public privacy information for Future Education and an overarching Future Projects privacy statement. Keeping it within this framework means the policy, school-specific arrangements and privacy information are maintained together. Future Education must make its privacy notices freely available at all times, including through the school website. Part C may also be published or linked separately if that makes the privacy information easier for Students, parents/carers, staff or Governors to find. A short, Easy Read or other accessible version should be provided where this helps a Student understand.

C1. General Future Projects privacy statement

The NR5 Project, trading as Future Projects, is a Norfolk charity delivering Future Education, Future Support, Future Radio and central charitable functions. Future Projects is normally the data controller where it decides why and how personal information is used. We use personal information only where we have a lawful purpose, keep it secure, limit access to people who need it, keep it only for as long as necessary and share it only where there is a lawful and proportionate reason.

This is the overarching Future Projects privacy statement. Because different services process different information for different purposes, additional service-specific privacy information may still be needed where this statement does not give an individual enough information about a particular use of their data. The notices below provide the detailed privacy information for Future Education.

Privacy point	Future Projects position
Controller	The NR5 Project, trading as Future Projects.
Contact	The Baseline Centre, 65–67 Knowland Grove, Norwich, NR5 8YD.
Data Protection Officer / Lead	Laura Knight, Finance & Business Support Officer – l.knight@futureprojects.org.uk.
What we use information for	To deliver charitable and educational services; support and safeguard people; employ and manage staff and volunteers; run governance, finance and fundraising; manage contracts, premises, technology, security and communications; meet legal/regulatory duties; respond to complaints, incidents and rights requests; and evaluate/improve services.
How long we keep it	In accordance with the retention schedules in this document and any service-specific statutory, contractual or safeguarding requirements.
International transfers	Only where an approved supplier or arrangement has an appropriate UK GDPR transfer mechanism and safeguards. Further details are available from the DPO.
Questions or concerns	Contact the DPO. You may also complain to the Information Commissioner's Office (ICO).

C2. Child-friendly Future Education privacy summary

For Students: This is the short version. The full Student/parent/carer privacy notice is in section C3. You can ask a member of staff, your parent/carer or the DPO to explain anything in another way.

Question	Answer
What information do we have?	Things such as your name and contacts, attendance, learning and exam information, EHCP/SEND needs, health information we need to support you, behaviour and pastoral records, safeguarding information, photos where appropriate, and information from school devices/networks.
Why do we use it?	To teach and support you, help you make progress, keep you safe, meet your SEND and health needs, communicate with you and your family, arrange exams and destinations, and meet the school's legal duties.

Question	Answer
Who can see it?	School staff only where they need it for their job. We may also need to share information with your local authority, health/social-care or safeguarding professionals, exam bodies, the Department for Education or other organisations where the law or your support requires it.
Do we sell it?	No. We do not sell Student information.
Do we use AI?	Only approved tools may be used. Staff must not put your identifiable information into public or unapproved AI tools.
Is school internet use monitored?	Yes. School networks/devices use filtering and monitoring to help keep Students and systems safe. Access to alerts is restricted to authorised people.
How long do we keep it?	It depends on the record. Some important school and safeguarding records are kept until you are 25; some records must be kept longer. See B10 for the full schedule.
Can I ask about my information?	Yes. You can ask what we hold, ask us to correct something that is wrong and use other data-protection rights where they apply. Ask the DPO or a member of staff for help.
Who can I talk to?	Laura Knight, Future Projects' Data Protection Officer and Data Protection Lead: l.knight@futureprojects.org.uk.

C3. Future Education privacy notice – Students, parents and carers

Last reviewed: September 2026. This notice applies to personal information used by Future Education about Students and, where relevant, their parents/carers and family members.

C3.1 Who is responsible for the information?

Future Education is operated by The NR5 Project, trading as Future Projects. Future Projects is normally the data controller because it determines why and how the school uses personal information. The school's Governing Body provides scrutiny and assurance but is not a separate controller merely because it governs the school.

The Data Protection Officer and Data Protection Lead is Laura Knight: l.knight@futureprojects.org.uk, The Baseline Centre, 65–67 Knowland Grove, Norwich, NR5 8YD.

C3.2 What information do we use?

- Identity and contact information for Students, parents/carers and emergency contacts.
- Admissions, attendance, timetables, curriculum, learning, progress, attainment, qualifications and post-16 destination information.
- SEND, EHCP, disability, accessibility and reasonable-adjustment information.
- Health, medical, medication, dietary, allergy and welfare information needed to support Students safely.
- Safeguarding, child-protection, pastoral, behaviour, positive handling/restrictive-intervention and risk information where relevant.
- Family, social-care, local-authority, placement, commissioning and professional reports relevant to education and support.
- Photographs, video or audio where needed for approved educational, safeguarding, administrative or publicity purposes.
- Examination, assessment and access-arrangement information.
- School IT, network, account, security, filtering and monitoring information.
- Complaints, incidents, accidents, correspondence, consent/preferences and records of decisions or disclosures.
- Other information we are required to collect by law, regulation, an awarding body or a lawful commissioning arrangement.

C3.3 Where does the information come from?

We may receive information directly from Students and parents/carers and from other sources where lawful and relevant, including previous or next education settings, local authorities, health and social-care professionals,

safeguarding agencies, examination/awarding bodies, the Department for Education, approved service providers and information created by school staff through teaching, assessment, safeguarding and pastoral work.

C3.4 Why do we use it and what makes this lawful?

Area	What we use it for	Typical lawful basis
Education and progress	To admit Students, plan and deliver education, assess progress, provide qualifications and prepare Students for next steps.	Legal obligation; contract where applicable; legitimate interests.
SEND and support	To understand needs, implement EHCP provision, make reasonable adjustments and coordinate appropriate support.	Legal obligation; legitimate interests; special-category conditions under UK GDPR/DPA 2018.
Safeguarding and welfare	To protect children, identify risk, record concerns, share information where necessary and work with safeguarding agencies.	Legal obligation; vital interests; legitimate interests; substantial public interest/safeguarding conditions.
Health and safety	To manage medical needs, medication, risk assessments, accidents, visits and emergencies.	Legal obligation; vital interests; legitimate interests; appropriate special-category conditions.
Attendance and regulation	To maintain required registers, support attendance, respond to absence and meet regulatory/inspection duties.	Legal obligation; legitimate interests.
Exams and destinations	To enter Students for qualifications, arrange access arrangements and support progression.	Legal obligation or legitimate interests; contract where applicable.
Communications	To communicate with Students, families, professionals and commissioners about education, welfare and school administration.	Legal obligation; legitimate interests; contract where applicable.
Security and online safety	To protect accounts, devices, networks and people; filter harmful content; monitor safeguarding/security risks; investigate misuse.	Legal obligation; legitimate interests; substantial public interest where safeguarding is involved.
Optional publicity	To use selected images, stories or other information for optional publicity where there is a genuine choice.	Consent where appropriate; otherwise another documented lawful basis.
Claims, complaints and accountability	To investigate complaints/incidents, manage legal claims, respond to rights requests, audit practice and demonstrate compliance.	Legal obligation; legitimate interests; legal claims conditions where relevant.

Where special-category or criminal-offence information is used, Future Projects also identifies an additional condition under Article 9/10 of UK GDPR and the Data Protection Act 2018. Depending on the purpose this may include safeguarding, substantial public interest, legal claims, employment/social protection, health/social care where applicable or explicit consent where it is genuinely appropriate. The detailed lawful basis is recorded in our record of processing activities.

Where we rely on legitimate interests, these may include delivering safe and effective education/support, protecting people and systems, managing communications, improving services and defending legal claims. We balance those interests against the rights and interests of the people affected.

C3.5 Do you have to give us the information?

Some information is required so the school can admit and educate a Student safely, meet safeguarding/attendance duties, provide SEND support, make statutory or regulatory returns, enter examinations or comply with lawful commissioning arrangements. If required information is not provided, the school may be unable to carry out the relevant duty or provide the service safely. Optional consent-based uses are not a condition of receiving education.

C3.6 Who do we share information with?

- Norfolk County Council and other local authorities or commissioners where they place, fund, support or have statutory responsibilities for a Student.
- The Department for Education and other education authorities through statutory or other lawful collections that apply to registered independent schools, including the School-level Annual School Census (SLASC).
- Previous or next schools, colleges and education/training providers where information is needed for a safe and effective transition.
- Examination boards, awarding organisations and approved education providers.
- Health, social-care, safeguarding and early-help services, the police and other statutory agencies where necessary and lawful.
- Approved IT, MIS, safeguarding, filtering/monitoring, communication, examination and other service providers acting under contract.
- Insurers, legal advisers, auditors, regulators, inspectors and professional advisers where necessary.
- Emergency services or others where needed to protect life or respond to a serious incident.

We do not sell Student or family personal information. Regular or sensitive sharing is governed by contracts, data-sharing arrangements or other documented controls where appropriate.

C3.7 Information shared with the Department for Education

Registered independent schools must complete statutory Department for Education collections that apply to them. Future Education provides the information required by those collections, including the School-level Annual School Census (SLASC), which covers matters such as Student and teaching numbers, courses of study, SEND, looked-after children and school/proprietor information. Other DfE collections or data-sharing arrangements will only be used where they apply to Future Education and have a lawful basis. The DfE becomes responsible for information it receives for its own purposes.

C3.8 Filtering and monitoring

Future Education uses filtering and monitoring on school networks and managed devices to help protect Students, staff and systems. The systems record or analyse internet/network use, attempts to access blocked or harmful content and security or safeguarding alerts. Depending on the approved system and configuration, relevant search terms or device activity may also contribute to alerts. Access to alerts and reports is restricted to authorised school safeguarding/senior staff, IT staff and approved providers who need it for their role.

Filtering and monitoring information is normally retained for the period in B10 (normally 12 months for routine logs). Where an alert becomes part of a safeguarding or incident record, that evidence follows the longer retention period for that record. The school reviews filtering and monitoring at least annually and completes a DPIA for new or materially changed monitoring where required.

C3.9 AI and EdTech

Future Education may use approved educational technology and AI tools where they support education or administration and have been appropriately assessed. Identifiable Student, parent/carer, staff, safeguarding or other restricted information must not be entered into public or unapproved AI tools. Where an approved AI/EdTech tool processes personal information, we assess the supplier, security, data use, retention, international transfers, model training, age restrictions, safeguarding and the need for a DPIA. We do not routinely make solely automated decisions with legal or similarly significant effects about Students.

C3.10 How long do we keep information?

The detailed school retention schedule is at B10. Core secondary-age Student records are normally retained until the Student's 25th birthday. Child-protection records are normally retained to age 25, with records relating to child sexual abuse retained longer in accordance with the schedule. Other records have shorter or longer periods depending on law, safeguarding, insurance, claims, exams and operational need. Destruction is suspended during a legal hold, active complaint, rights request, investigation or claim.

C3.11 International transfers and suppliers

Some approved cloud or technology suppliers may store or make information accessible outside the UK. Future Projects only permits this where an appropriate UK GDPR transfer mechanism and safeguards are in place. Supplier statements alone are not treated as sufficient where formal safeguards are required. Further information about a particular supplier or safeguard can be requested from the DPO.

C3.12 Your rights

Depending on the circumstances and lawful basis, individuals may have rights to be informed, access their information, correct inaccurate information, ask for erasure or restriction, object to processing, receive portable information and obtain safeguards in relation to automated decision-making. Some rights are limited where the school must keep or use information to meet a legal, safeguarding or other overriding requirement.

Where processing is based on consent, consent can be withdrawn at any time for future use. Withdrawal does not make earlier lawful processing unlawful. A child who is competent to understand the request can exercise their own rights; otherwise an appropriate person with parental responsibility may act where this is in the child's best interests.

Right to object: Where Future Projects relies on legitimate interests, you have the right to object. We will consider the objection and stop the processing unless we can demonstrate compelling legitimate grounds or the processing is needed for legal claims.

C3.13 Questions and complaints

Contact Laura Knight, Data Protection Officer and Data Protection Lead, at l.knight@futureprojects.org.uk. We will handle data-protection complaints under Part A. You also have the right to complain to the Information Commissioner's Office (ICO): ico.org.uk, telephone 0303 123 1113, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

C4. Future Education privacy notice – workforce

This notice applies to applicants, current and former employees, agency workers and other school workers where Future Education/Future Projects processes their personal information in connection with work at the school.

Privacy point	Workforce notice
Information we use	Identity/contact details; application and employment history; references; right-to-work and safer-recruitment checks; DBS and barred-list information where lawful; qualifications and professional information; contract, role and pay; bank, tax, pension and payroll information; leave and attendance; training, appraisal and performance; health, disability and adjustments; equality monitoring; safeguarding, disciplinary and grievance information; accidents/incidents; IT/account/security logs; emergency contacts; and work communications/records.
Where it comes from	The individual; referees; recruitment agencies; DBS and government services; professional/regulatory bodies; occupational-health providers; managers; payroll/pension providers; IT/security systems; safeguarding agencies; and other lawful sources relevant to the role.
Why we use it	Recruitment and safer recruitment; entering into and managing employment/engagement; paying staff and administering benefits/pension; training, performance and workforce planning; attendance, leave and adjustments; health and safety; safeguarding; security and acceptable use; complaints/disciplinary/grievance;

Privacy point	Workforce notice
	equality monitoring; legal/regulatory reporting; claims, audit and organisational assurance.
Lawful bases	Contract and steps before contract; legal obligations; legitimate interests; vital interests in emergencies; and consent only where there is a genuine choice. Special-category data uses an appropriate Article 9/DPA 2018 condition, including employment/social protection, occupational health where applicable, safeguarding/substantial public interest, equality monitoring, legal claims or explicit consent where appropriate.
Who we share it with	HMRC; pension/payroll providers; DBS and relevant government bodies; DfE or other statutory education collections where applicable; local authorities/commissioners where required; occupational health; professional/regulatory bodies; insurers/legal advisers; safeguarding agencies/police where lawful; approved HR/IT/payroll providers; auditors and regulators.
Monitoring	Work accounts, devices, networks and systems may be logged or monitored where lawful, necessary, proportionate and transparent for security, safeguarding, compliance and investigation. Monitoring is not used as unrestricted surveillance.
Retention	The general staff personnel file is normally retained for 6 years after employment ends. DBS certificate copies are normally kept no longer than 6 months after the recruitment decision. Safeguarding allegations and other specialist records follow the longer periods in the retention schedules.
Rights and complaints	The rights in C3.12 apply according to the lawful basis. Questions and complaints should be sent to the DPO; the right to complain to the ICO also applies.

C5. Future Education privacy notice – governors and governance roles

This notice applies to members of the Future Education Governing Body and other people whose information is processed because of a school governance role.

Privacy point	Governance notice
Information we use	Identity and contact details; role/term of office; appointment and eligibility information; declarations of interests; training; attendance; meeting/minute records; correspondence; safeguarding/DBS information where lawful and relevant; skills/experience; photographs or biographies where used; and information required for regulatory/governance records.
Why we use it	To appoint and support Governors; communicate; manage meetings and decisions; record accountability; manage conflicts; support safeguarding and safer governance; provide training; comply with regulatory, inspection and statutory information requirements; and maintain the governance archive.
Lawful bases	Legal obligations and legitimate interests in effective and accountable governance. Special-category/criminal information uses an appropriate additional condition where required.
Who we share it with	Future Projects Trustees and staff where necessary; DfE and other education/regulatory bodies where required; inspectors; local authorities/commissioners where lawful; auditors/legal advisers; safeguarding bodies where necessary; and the public where governance information is required or appropriately published.
Retention	Approved governance minutes and key governance records are permanent. Routine working papers are normally retained for 6 years after they are superseded or no longer required, unless a longer legal, safeguarding or governance need applies.
Rights and complaints	The rights in C3.12 apply according to the lawful basis. Questions and complaints should be sent to the DPO; the right to complain to the ICO also applies.

C6. Review, accessibility and changes

The DPO will review the privacy information at least annually and whenever Future Projects or Future Education makes a significant change to how personal information is used. Significant changes will be brought to the attention of the people affected before or when the new use begins where required.

The school will keep the privacy notices freely available. Students will be offered explanations in an age-appropriate and accessible form and reasonable adjustments will be made for SEND, communication, literacy or other needs. This document can be published in full, while Part C may also be extracted or linked separately where that makes the privacy information easier to find.

Part D. Organisation-wide appendices

Appendix A. Information classification and handling matrix

The classification is determined by sensitivity and the likely impact of inappropriate access, alteration, loss or unavailability. Personal data may fall into more than one level depending on context. Where uncertain, use the higher classification and seek advice.

Classification	Examples	Minimum handling requirements
Public	Published policies, approved publicity, public website content, published reports and information explicitly authorised for public release.	May be shared openly after accuracy, copyright, consent and approval checks. Protect approved versions from unauthorised alteration.
Internal	Routine internal procedures, meeting arrangements, general staff communications and operational information not intended for public release.	Use approved systems. Share only for legitimate organisational purposes. Do not post publicly without authority.
Confidential	Most personal data; service-user contact information; personnel, finance, contracts, donor, incident and case-management information; commercially sensitive information.	Need-to-know access; approved systems and devices; secure transfer; locked paper storage; no personal email or consumer cloud; secure disposal.
Restricted	Safeguarding records; Student and special-category records; criminal-offence and DBS information; credentials; high-risk financial data; legal advice; security configurations; serious incident and breach investigations.	Strict role-based access; minimum necessary copies; enhanced authentication and secure transfer; no local or personal-device storage; log or record significant disclosure; DPO, DSL or IT advice where appropriate.

Handling rule

The classification applies to the information, not simply the file name or system. A routine email may become Restricted if it contains safeguarding information or credentials. Information should be declassified or anonymised only by an authorised person.

Appendix B. Privacy screening and DPIA process

B1. Initial screening questions

The project or service manager should answer the following before procurement, contracting, design or collection begins:

- What is the purpose and expected benefit, and is personal data genuinely necessary?
- Whose information will be used, including children or people who may be vulnerable?
- What categories and volumes of information are involved, including health, safeguarding or criminal-offence data?
- Where will information come from and how will people be informed?
- Which lawful bases and special-category or criminal-offence conditions apply?
- Who will access or receive the information and what controller or processor roles apply?
- Which systems, suppliers, devices and locations will be used, including any access outside the UK?
- Will data sets be linked, monitored, profiled, scored or used with AI or innovative technology?
- What could go wrong and what harm could occur?
- How will accuracy, minimisation, access, security, retention, rights, complaints and deletion be managed?
- Can the objective be achieved with less information or a less intrusive method?

B2. DPO review and advice

The DPO advises whether a full DPIA is legally required, advisable as good practice, or unnecessary. The responsible manager records the outcome and rationale on the privacy-screening or DPIA register.

B3. Full DPIA contents

1. Describe the processing, purpose, context, systems, people, flows, recipients, retention and roles.
2. Explain necessity and proportionality, lawful bases, transparency, minimisation, accuracy, rights and alternatives.
3. Record consultation with staff, partners, specialists and people affected where appropriate.
4. Identify risks to people, including discrimination, loss of control, financial loss, safeguarding harm, distress and exclusion.
5. Assess likelihood and severity before controls.
6. Specify technical and organisational controls, owners and completion dates.
7. Reassess residual risk and determine whether prior ICO consultation may be required.
8. Record DPO advice, the management approval/go-live decision, any conditions and the review date.

B4. Approval and review

The manager remains accountable for the processing decision and for implementing controls. The DPO provides independent advice on the data protection assessment. The IT Manager confirms technical controls where relevant. The CEO decides any significant residual-risk matter. The DPIA must be reviewed when the processing, supplier, data, purpose, access, technology or risk materially changes and after relevant incidents or complaints.

Appendix C. Personal data breach action card

Immediate rule

Report every suspected personal data breach immediately to Laura Knight, Data Protection Officer, and report cyber-related incidents to the IT Manager. Do not wait for certainty or complete information.

1. PROTECT people and stop further disclosure or loss where safe to do so.
2. REPORT immediately to the DPO and, for cyber or system issues, the IT Manager. Notify the relevant manager.
3. PRESERVE evidence. Do not delete messages, wipe devices, alter logs, reset equipment or conduct an unauthorised investigation.
4. CONTAIN under DPO or IT instruction: recall messages, revoke links, restrict permissions, isolate devices or accounts, recover papers or contact the unintended recipient.
5. RECORD what happened, when it was discovered, information and people affected, systems or recipients involved and actions already taken.
6. ASSESS risk and notification requirements. The DPO leads the assessment and documents the decision.
7. RECOVER and learn through secure restoration, communication, support, corrective action and post-incident review.

Issue	Immediate route
Immediate danger, crime in progress or serious medical emergency	Call 999, then follow internal escalation.
Safeguarding concern	Contact the relevant Designated Safeguarding Lead immediately and follow the safeguarding policy.
Phishing, malware, stolen account or device, system compromise	IT Manager and DPO immediately; follow Business Continuity cyber instructions.
Misdirected email, paper or disclosure	DPO and manager immediately; attempt safe containment without creating further disclosure.
Likely risk to rights and freedoms	DPO coordinates ICO notification without undue delay and, where feasible, within 72 hours.
Likely high risk to people	DPO and CEO coordinate clear notification to affected people without undue delay unless a lawful exception applies.

Appendix D. Records retention schedule

These are the default organisation-wide periods. A longer or shorter period may apply where legislation, a contract, insurance, safeguarding, education, professional guidance or a documented risk assessment requires it. For Future Education, the separate Future Education Data Protection & Information Governance: School-specific arrangements and records retention schedule contains the detailed Student and school record periods and takes precedence for those records. Destruction must be suspended during a legal hold, rights request, complaint, audit, investigation, claim or regulatory enquiry.

Record category	Default retention period	Notes and exceptions
Policies, governing documents, Trustee and Governor minutes, annual reports and final audited accounts	Permanent	Retain approved versions and key superseded versions as part of the governance archive.
Routine committee, management and project minutes	6 years after superseded or project closure	Longer where they evidence significant decisions, property, safeguarding or contractual obligations.
Accounting, tax, payroll and routine financial transaction records	6 years after the end of the relevant financial or tax year	Longer periods may apply to capital assets, property, pensions, grants, fraud or contractual requirements.
Contracts and procurement records	6 years after expiry or termination; 12 years where executed as a deed	Include material variations, approvals, due diligence and performance records.
Unsuccessful recruitment applications and interview records	6 months after recruitment closes	Longer only where a complaint, claim or explicit talent-pool consent applies.
Employee personnel files	6 years after employment ends	Specialist health, pension, safeguarding, DBS or education records may require different periods.
Training, competency and supervision records	Employment or role plus 6 years	Safeguarding and regulated-role evidence may be retained longer under specialist schedules.
DBS certificate information	Normally no longer than 6 months after the decision	Retain only the permitted check record and follow the DBS policy and Code of Practice.
Adult service-user case records	7 years after case closure or last meaningful contact	Longer where safeguarding, contract, limitation, litigation or continuing risk requires.
Student and child education records	See B10 Future Education schedule	The school-specific schedule in Part B takes precedence for Student records.
Adult safeguarding records	Specialist safeguarding schedule; normally at least 7 years after closure	Retain longer where allegations, continuing risk, legal action or statutory guidance requires.
Child safeguarding records	See B10 Future Education schedule	The school-specific safeguarding periods in Part B take precedence.
General incident, accident and near-miss records	6 years after closure	Child, safeguarding, RIDDOR, insurance or litigation records may require longer.

Record category	Default retention period	Notes and exceptions
Routine service-user complaints and compliments	3 years after closure	Serious complaints, claims, safeguarding or regulatory matters: 6 years or longer according to risk.
Data protection rights requests and complaints	6 years after closure	Retain request, searches, disclosure, decisions, correspondence and outcome securely.
Personal data breach and cyber incident records	6 years after closure	Material incidents may be retained longer for legal, insurance, security and organisational learning.
DPIAs, privacy screening, legitimate-interest assessments and transfer assessments	Duration of processing plus 6 years	Retain significant superseded versions and evidence that actions were completed.
Data-sharing agreements, processor due diligence and supplier assurance	Contract or sharing period plus 6 years	Longer for deeds, disputes, continuing liabilities or significant incidents.
Access, security and system logs	Normally 12 months	Longer where needed for security, safeguarding, audit, incident investigation or system requirements.
Visitor and routine building sign-in records	12 months	Longer where linked to an incident, safeguarding concern or security investigation.
CCTV recordings, where used	Normally 30 days	Extracts linked to an incident, claim, police or safeguarding matter follow the relevant record period.
Routine enquiries and contact correspondence	12 months after resolution	Transfer material decisions, consent or case information to the official record before deletion.
Fundraising, donor and supporter records	6 years after the last financial transaction or active relationship	Retain suppression and preference information as necessary to respect objections and legal duties.
Marketing consent and preference records	While relied upon and normally 6 years after last use	Suppression records may be retained longer where necessary to prevent unwanted contact.
Backups	Rolling schedule set by the IT Manager	Backups are for recovery, not archive; legal holds and secure expiration must be considered.

Secure disposal

At the end of the period, the responsible manager must confirm that no hold or exception applies. Paper goes to approved confidential waste; electronic information and media are securely erased or destroyed. Disposal of significant record sets should be documented.

Appendix E. BYOD user conditions

Authorised use of a personal phone to access Future Projects Outlook and Teams is conditional on all of the following:

Condition	Requirement
Authorisation	The IT Manager has approved the device and the user, and Company Portal is installed and compliant.
Permitted access	Outlook and Teams only by default. Other systems require separate written approval.
Device security	Supported operating system, security updates, secure screen lock, no rooting or jailbreaking, and no sharing of the unlocked device.
Corporate controls	The user accepts authentication, compliance checks, session revocation, blocking and removal of corporate access or work data.
No local storage	No downloading, copying, photographing, screen-recording or backup of personal, confidential or restricted information to personal storage or apps.
Approved communication	No forwarding to personal email, consumer messaging, personal cloud storage or unapproved applications.
Physical control	The device remains under the user's control and is not left unlocked or visible to others.
Incident reporting	Loss, theft, compromise, unexpected prompts or loss of control is reported immediately to the IT Manager and DPO.
Departure or role change	Corporate access is removed immediately and the user cooperates with removal of organisational information.
Withdrawal	Future Projects may restrict or withdraw access where risk, non-compliance, technical change or operational need requires.
Personal privacy	Future Projects will manage the corporate work environment and will not intentionally access personal content outside it; users remain responsible for personal backups and understanding device-management implications.

User responsibility

Use of BYOD does not transfer responsibility for organisational information to the device owner. Future Projects remains responsible for corporate data and may require immediate action to protect it. A personal device must never be the only location of a work record.