



MEPA TRAINING DATA PROTECTION POLICY

Applies to MEPA Academy, MEPA College and MEPA Studios

This policy sets the rules for collecting, using, sharing, securing and disposing of personal information across MEPA's education, training and performing arts provision in England. It protects learners, families, staff and other people whose information we handle, while supporting education, safeguarding and lawful administration.

Document control	Details
Version	October 2026 revision of the August 2026 policy
Legislation and guidance checked	10 October 2026
Policy owner and initial contact	Emma Finch — efinch@mepatraining.com
Approval status	Revised for proprietor approval; adoption has not been recorded
Approval and effective date	To be recorded by the proprietor
Next planned review	August 2027, or sooner following relevant changes
Approval record	Approver name and role: _____ Date: _____

Before adoption, complete Appendix B. Names and contact details are retained from the supplied policy; the legal controller identity and DPO arrangements must be verified. This policy establishes required practice and does not certify that every operational control is already in place.



1 Purpose and scope

All employees, self-employed teachers, contractors, volunteers, leaders and proprietors must follow this policy when handling MEPA information. It covers paper files, email, management systems, parent portals, cloud services, CCTV where used, recordings, photographs, devices and approved artificial intelligence tools. It applies to prospective, current and former pupils and students, parents and carers, applicants, employees, contractors, visitors and other contacts.

MEPA Academy, MEPA College and MEPA Studios may have different legal duties and contractual arrangements. The name “Academy” does not itself establish that a setting is a state-funded academy or public authority. We check each setting’s legal status before applying public-sector education duties, data returns, information rights or lawful bases. Sharing across MEPA brands is subject to the same purpose, access and transparency checks as other processing.

2 Legislation and guidance

We comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Privacy and Electronic Communications Regulations 2003 (PECR), as amended, including commenced provisions of the Data (Use and Access) Act 2025 (DUAA). The DUAA amends rather than replaces these laws. [1–4]

For the relevant setting and activity, we apply education, employment, equality, tax and safeguarding legislation, including the Education (Independent School Standards) Regulations 2014, Children Act 1989, Children Act 2004 as amended, and Protection of Freedoms Act 2012. We have regard to Keeping Children Safe in Education 2026, Working Together to Safeguard Children 2026 and the September 2026 Information Sharing Duty guidance. [5–7]

DfE’s data protection in schools guidance is used as a practical benchmark; its maintained-school and state-funded academy provisions are not automatically duties on independent provision. ICO guidance governs our interpretation of data protection requirements. Relevant guidance and source links are listed in Appendix C. [2]

3 Controller identity and responsibilities

The data controller is the legal organisation that determines why and how personal data is processed. Emma Finch is the named contact in the original document; this does not make her personally the controller. Before adoption, the proprietor must record the full legal name, registered or principal address, and controller relationship for each setting. Where separate entities jointly determine processing, we document an Article 26 arrangement and make its essence available to individuals.

Existing contact route: Emma Finch, MEPA Training, Earl House, 27 & 29 Earl Street, Maidstone, Kent, ME14 1PF; efinch@mepatraining.com. The proprietor must ensure this route is monitored during closure periods and provide a deputy route internally.

- The proprietor retains accountability, approves policy and resources, and receives reports on risks, incidents, complaints and overdue actions.
- The data protection lead maintains records of processing, notices, retention arrangements, rights and complaints logs, supplier checks, and staff guidance; obtains specialist advice when needed; and coordinates incident response.
- The designated safeguarding lead (DSL) controls safeguarding information, secure transfers and safeguarding disclosure decisions, working with the data protection lead or DPO without delaying protective action.
- Managers and system owners approve appropriate access, maintain accurate records, oversee disposal and implement supplier and security controls. All staff use approved processes and report incidents and requests promptly.

The proprietor must assess and record whether Article 37 requires a data protection officer (DPO), including public-authority status and core activities involving large-scale systematic monitoring or sensitive data. A DPO is not automatically required solely because an independent business provides education. If required, or voluntarily appointed as a DPO, the role must have expertise, resources, independence, no conflicting decision-making responsibilities and direct access to the highest management level. Publish the DPO's contact details and notify the ICO. Do not present an unconfirmed data protection lead as the statutory DPO. [8]

4 Principles and accountability

Personal information must be processed lawfully, fairly and transparently; collected for specified legitimate purposes; limited to what is needed; accurate and corrected promptly; kept only as long as necessary; and protected against unauthorised use, loss and damage. MEPA must be able to demonstrate compliance. Staff must distinguish facts, professional judgement and allegations and avoid irrelevant or stigmatising comments. [9]

We maintain a record of processing activities appropriate to Article 30, including purposes, people and data categories, recipients, lawful bases, sensitive-data conditions, overseas transfers, retention rules and security measures. The small-organisation exemption must not be assumed for regular learner or workforce processing. We also retain consent records, legitimate interests assessments, data protection impact assessments (DPIAs), sharing decisions, processor contracts, training records and rights, complaints and breach logs.

5 Information we collect and why

We collect information directly from individuals and, when lawful, from previous education providers, parents and carers, local authorities, health or social care professionals, awarding organisations, referees and government bodies. We explain required and optional fields, the reason for collection, and the practical consequences of not providing required information. We do not collect nationality, country of birth, ethnicity, driving licences or other documents merely because a system has a field for them.

Learners and families

Relevant records may include identity and contact details; dates of birth; parent or carer details and parental responsibility; emergency contacts; applications and waiting lists; attendance and absence reasons; progress, assessments and qualifications, including BTEC and IDTA where applicable; conduct, suspensions and exclusions; SEND, EHC plans and support; physical and mental health, allergies and medical provision; safeguarding; performance licensing; fees and payments; communications; and photographs or recordings for defined purposes.

We use these records to administer admissions, education and classes; support learning, assessment and examination entries; monitor attendance and progress; provide adjustments and pastoral care; safeguard welfare; organise performances and trips; meet applicable licensing, regulatory and reporting duties; manage fees and contracts; and review provision. Optional promotion is managed separately from core provision.

Workforce and other contacts

Relevant workforce records may include identity, contact and emergency details; recruitment applications, references and qualifications; right-to-work and safer recruitment checks; DBS check information; contracts and self-employment arrangements; hours, roles, leave and pay; National Insurance, tax, bank and pension details; appraisal, grievance and disciplinary information; sickness and adjustments; and proportionate IT security records. We use them for recruitment, engagement, payroll, safeguarding, employment administration, legal compliance and service management. Visitor and supplier records support site security, contact and procurement.

Sensitive information may include health, racial or ethnic origin, religious beliefs, trade union membership, sexual orientation or political opinions. It is collected only where a specific purpose and lawful condition justify it. Criminal allegations, convictions and DBS information require separate Article 10 safeguards.

6 Lawful bases

Before processing, we select and record the lawful basis for each purpose and controller. A general reference to the Education Act 1996 or Children Act 1989 is not a sufficient basis for all MEPA activities. We rely on a legal obligation only where the identified duty actually applies; public task requires a function or authority grounded in law. [10]

Basis	How it may apply
Legal obligation Article 6(1)(c)	Processing necessary for an applicable duty, such as payroll reporting, right-to-work checks, safeguarding or a required education return. Identify the specific duty.
Contract Article 6(1)(b)	Necessary steps for a contract with the individual or pre-contract steps they request. A parent's fee contract does not automatically justify processing their child's data under this basis.
Legitimate interests Article 6(1)(f)	Necessary private-provider administration or security, subject to a recorded purpose, necessity and balancing assessment giving particular weight to children's interests. Not for public authorities performing their public tasks.
Recognised legitimate interests Article 6(1)(ea)	Only a qualifying Annex 1 purpose, such as safeguarding children or at-risk adults, meeting all conditions. Document necessity. It is not a general education or marketing basis.
Public task Article 6(1)(e)	Only processing necessary for an actual legally grounded public-interest task or official authority; identify that law and the relevant setting.
Consent Article 6(1)(a)	Genuine optional uses, including the promotional images policy below. Freely given, specific, informed, affirmative and withdrawable without detriment.
Vital interests Article 6(1)(d)	Necessary protection of someone's life, such as an emergency; not a routine medical or safeguarding basis.

Recognised legitimate interests removes the balancing test for the prescribed purposes but does not remove the necessity test, transparency, security or sensitive-data requirements. It cannot support solely automated significant decisions. Public authorities cannot use it for their public tasks. We check the adult safeguarding conditions separately for learners aged 18 or over. [11]

Special category and criminal offence information

Special category processing needs both an Article 6 basis and an Article 9 condition. Possible conditions include employment and social protection obligations under Article 9(2)(b), substantial public interest under Article 9(2)(g) with the relevant DPA Schedule 1 condition, or lawful health or social care under Article 9(2)(h) where its requirements are met. A school is not automatically a health-care provider. Explicit consent is used only where valid and appropriate. [10]

For safeguarding, we consider the safeguarding of children and individuals at risk condition in DPA Schedule 1, paragraph 18, and its requirements for processing without consent. We maintain an appropriate policy document where the chosen condition requires one. Criminal offence information needs an Article 6 basis and Article 10 authorisation through UK law, including a suitable DPA condition where required. Access to these records is tightly restricted.

7 Transparency and privacy notices

This internal policy does not replace an Article 13 or 14 privacy notice. We provide accessible, age-appropriate notices for learners and families, workforce and applicants, and other relevant groups. Notices identify the actual controller and DPO where appointed, purposes and lawful bases, legitimate interests where used, recipients, retention periods or criteria, transfers and safeguards, rights and complaint routes. They explain mandatory information and any significant automated decisions. [12]

Provide the notice when collecting data directly. For data obtained elsewhere, provide the required information within one month, or earlier on first contact or disclosure, unless a documented legal exception applies. Identify the source and categories. Inform people before a materially different use begins; assess compatibility and lawful basis first. Appendix A preserves the original notice content as requirements for updated notices, rather than presenting unverified operational statements as a final public notice.

8 Children and family access

Data protection rights belong to the child. We assess understanding and maturity case by case; there is no universal age of 12 or 13 at which parents lose or gain access. For a parent acting on a child's behalf, verify identity, authority and whether the child understands and authorises the request or lacks competence. Consider the child's wishes, confidentiality, court orders and potential harm. A fee payer or portal account holder is not automatically entitled to all records. [27]

For college students aged 18 or over, parents normally receive information only with the student's authority or another documented lawful justification. Emergency contacts do not have unrestricted access. We maintain separate family contacts and access permissions, taking account of separated parents and safeguarding restrictions. Statutory educational-record access rights depend on the type of setting; the maintained-school 15-school-day rule must not be applied automatically to MEPA's independent provision.

Where a directly offered online service to a child relies on consent, the UK GDPR age threshold of 13 applies in the relevant circumstances. It does not determine consent for all school activities. We assess whether a service falls within the Children's Code and relevant child-focused online-service requirements before deployment.

9 Safeguarding and information sharing

Staff must share safeguarding concerns promptly through the DSL and established referral procedures. Data protection is not a reason to delay protection. Consent is not usually the appropriate basis for essential safeguarding disclosures. Use a lawful basis and any required sensitive-data condition; share relevant, accurate information securely and record the decision. [5]

The information sharing duty under section 16LA of the Children Act 2004 commenced on 30 September 2026. For organisations and recipients within scope, relevant child or connected-person information must be disclosed so far as sharing may facilitate the recipient's safeguarding or welfare functions, including early support. A significant-harm threshold is not required. The duty is qualified where disclosure would be more detrimental to the child than non-disclosure. The DSL records scope, relevance, recipient, any mitigation and reasons for withholding; parental objection or absent consent alone does not displace the duty. Determine each MEPA setting's inclusion in the statutory scope. [6]

We remain transparent with families unless informing them would create risk or prejudice protective action. Keep child protection records separate from general learner records and transfer them securely to the receiving DSL in accordance with current KCSIE, with receipt confirmed. Local safeguarding arrangements under Working Together guide multi-agency working. [5,7]

10 Other sharing and suppliers

We share only information required for a defined lawful purpose. Potential recipients, where relevant, include receiving education settings, Kent County Council and other responsible authorities, DfE, health and social care services, police and courts, awarding organisations, performance licensing bodies, inspectors or regulators with applicable powers, professional advisers, insurers, payroll and pension providers, and approved IT suppliers. Membership of ISA or CDMT does not itself establish a statutory right to receive personal information. Families and representatives receive information only where authorised or otherwise lawful.

Verify a requester's identity and authority, document the basis, check necessity and use secure transfer. A request from police or another public body does not automatically require the release of a complete file. Routine sharing agreements set out purpose, roles, security, retention and rights; absence of an agreement must not obstruct urgent lawful safeguarding sharing.

Before appointing a processor, assess security, subcontractors, retention, access, incident assistance and overseas handling. Article 28 contracts require processing on documented instructions, confidentiality, appropriate security, authorised subprocessors, help with rights and breaches, return or deletion at the end of service, and audit information. Check whether a supplier also processes information independently for its own purposes. [14]

11 Security and access

Use named accounts and the minimum access needed for the role. Apply multifactor authentication where available, especially for remote access, email and privileged accounts. Review permissions when duties change and remove access promptly on departure. Restrict safeguarding, medical, SEND, HR and financial files separately; log and review access and exports where appropriate.

Use approved encrypted devices and secure transfer methods, patch software, protect backups and test restoration. Paper records must be locked away and transported securely. Staff must check recipients and attachments, use appropriate bulk-email controls, lock screens, protect passwords and avoid unattended printed records. Personal email, unapproved cloud storage and unapproved messaging must not be used for MEPA personal data. Remote work and personal-device access require approved safeguards.

For parent portals and linked systems, verify relationships and enforce authorisation on the server, not just through hidden buttons or email matching. Check exports, downloadable reports, shared links and integrations so users cannot retrieve another family's records. System changes must undergo access and disclosure checks before live use.

12 Retention and secure disposal

There is no UK GDPR rule that all student information must be held to age 25. We use an approved schedule that records each record type, purpose, legal or business justification, retention trigger, duration, owner and disposal method. An age-25 period may be appropriate for specified pupil records, but must not be extended to every record or all Studios and College data. [15]

Separate education files, safeguarding, SEND, attendance, examination, employment, financial, licensing, complaints, images and CCTV records. Apply relevant statutory rules and current sector recommendations to the actual setting. Retain only necessary recruitment-check evidence; DBS certificate copies are normally destroyed within six months unless a longer period is properly justified, while the required check record is retained. [5]

Suspend routine destruction for a live request, complaint, investigation, legal claim or applicable preservation requirement, documenting the hold and reviewing it. Review records at the scheduled trigger, erase electronic data securely and shred confidential paper. Manage supplier copies and

backup expiry, and avoid restoring deleted records to active use. Keep evidence of disposal; do not claim a retention schedule is complete until approved.

13 Individual rights and subject access

People may request access, correction, erasure, restriction, portability where applicable, or object to processing. Rights depend on the basis and circumstances: erasure is not absolute, portability principally concerns automated consent or contract processing, and an objection to direct marketing must be honoured. Staff forward any request to the data protection lead immediately, whatever channel is used. We record receipt, decisions and deadlines. Respond to rights requests without undue delay and normally within one calendar month, applying only lawful extensions or exceptions. [16]

For a subject access request, respond without undue delay and normally within one calendar month. School holidays do not suspend the deadline. A necessary extension of up to two further months for complexity or multiple requests must be explained within the initial month. Requests need no special form and are normally free. Verify identity proportionately and disclose securely. [13]

Make reasonable and proportionate searches, recording systems, date ranges and reasons. Clarification may pause the statutory clock only where reasonably necessary to identify the information or processing activities covered, following current ICO rules; explain the pause and record the recalculated deadline. Do not require narrowing of an already clear request. [17]

Assess third-party information and exemptions individually, including relevant education, health, social work and serious-harm provisions. Do not refuse an entire safeguarding file simply because it is sensitive. Redact where justified and provide the remaining data and supplementary information. A manifestly unfounded or excessive request may be refused or charged for only where the legal test is met and reasons are documented. Explain any refusal, the ICO complaint route and judicial remedy within the applicable deadline. [27]

14 Data protection complaints

Since 19 June 2026, controllers must provide a way to complain directly about data protection. Complaints may be made to Emma Finch through the contact route in section 3, verbally to a member of staff or by letter or email. Staff record and forward them promptly. A complaint form may help but is not compulsory, and reasonable adjustments must be provided. [18,19]

Acknowledge receipt within 30 days. Begin appropriate enquiries on receipt, investigate without undue delay and keep the person informed. Give an outcome without undue delay, explaining findings, reasons, remedies and the right to complain to the ICO. The 30-day period is for acknowledgement, not a statutory final-response deadline. Keep a proportionate complaint record and use findings to improve practice. [18]

An uninvolved senior leader or the proprietor reviews complaints about the named contact; obtain independent advice where needed. A complaint involving a breach triggers the incident process immediately. A rights request within a complaint retains its own deadline. People may contact the ICO at ico.org.uk/make-a-complaint/ or 0303 123 1113; our process does not remove that right.

15 Personal data breaches

A breach can involve confidentiality, accuracy or availability, including lost files, misdirected email, unauthorised portal access, accidental deletion or ransomware. Staff report suspected incidents immediately to the data protection lead and relevant senior leader; use the DSL route if there is a safeguarding risk. Do not wait for proof or for normal opening hours. [20]

Contain the incident safely, preserve evidence, recover or restrict access where possible, and record when MEPA became aware, what happened, data and people affected, possible harms and mitigation.

The controller assesses whether notification is required, with DPO advice where available. Report to the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to risk individuals' rights and freedoms. Explain delay and provide phased information if necessary. [20]

Notify affected people without undue delay where a breach is likely to result in a high risk, unless a specific legal exception applies. Keep a record of every breach and notification decision, including non-reporting. Processors must tell MEPA without undue delay. Implement lessons and review controls; make other regulatory, police, contractual or safeguarding reports where applicable.

16 Technology and high risk processing

Build data minimisation, access restrictions and retention into new processes and settings. Complete a DPIA before processing likely to cause high risk, including relevant surveillance, biometrics, sensitive-data systems, profiling or innovative technology involving children. Assess purpose, necessity, proportionality, risks and safeguards, consult the DPO where appointed and seek ICO prior consultation if high residual risk cannot be reduced. [12]

Artificial intelligence and automated decisions

Staff must not put identifiable learner, family, workforce, SEND or safeguarding information into public or unapproved AI tools. Before approval, examine the provider's purposes, model training, storage, deletion, security, subprocessors, transfer arrangements and accuracy. Minimise or effectively anonymise inputs, provide transparency and complete a DPIA where required. Removing names alone may not anonymise a record. [21]

MEPA requires meaningful human decision-making for admissions, exclusions, safeguarding action and other decisions affecting access to education or support. Automated scores or alerts may assist but must be checked for accuracy and fairness. If future solely automated significant decisions are proposed, obtain legal review and meet the amended UK GDPR requirements, including stricter special-category rules and safeguards to provide information, allow representations, human intervention and challenge. Do not use recognised legitimate interests for such decisions. [11,22]

International transfers

Check whether overseas hosting, subprocessors or remote access create a restricted transfer. Use applicable UK adequacy regulations or an appropriate safeguard such as the UK IDTA or UK Addendum, with the required data protection test. The test considers whether protection after transfer is not materially lower than in the UK, acting reasonably and proportionately. Document the assessment and extra safeguards. Routine cloud use must not rely casually on exceptional derogations. Privacy notices explain transfers and how safeguards may be obtained. [23]

17 Images marketing CCTV and biometrics

For optional promotional photographs, videos, social media and publicity, MEPA's policy is to obtain specific consent from the appropriate person, taking account of the learner's competence and wishes. Separate permissions by purpose and channel; refusal must not disadvantage a learner. Keep current permissions accessible to authorised staff, check safeguarding restrictions and offer ways to participate without being publicised. Explain wider internet sharing and its risks. Identity or assessment images may use another appropriate basis; a photograph is not automatically biometric special-category data. [24]

Withdrawal stops future consent-based use and prompts removal from channels we control where practicable; explain limitations for already distributed print or third-party republication. Personal family

photography for domestic use is treated differently from MEPA's official use, subject to event and safeguarding rules.

Administrative messages must be distinguished from marketing. For marketing email or text to individual subscribers, obtain PECR-compliant consent unless a documented applicable soft opt-in meets every condition. Always identify the sender and provide a simple opt-out, maintaining a minimal suppression record. Do not assume that a contact for Academy administration permits Studios or College marketing. The charitable-purpose soft opt-in is available only to qualifying charities and where its conditions are met. [25]

Website cookies and similar technologies require consent unless a current PECR exception applies. Document any DUAA exception and meet its conditions, including transparency and any required objection mechanism. Advertising and non-exempt tracking must not be activated before valid consent. Refusal and withdrawal must be easy.

If CCTV is used, document purpose, lawful basis, necessity, coverage, access and a justified short retention period. Display notices and process disclosure requests lawfully. Do not install it in toilets or changing facilities, and do not enable routine audio recording without exceptional justification and approval. [24]

Before any automated biometric recognition of children under 18 at a school or college, follow Protection of Freedoms Act duties: notify parents, obtain written consent from at least one parent subject to statutory exceptions, respect any parent's written objection and the child's objection or refusal, and offer a reasonable alternative without disadvantage. Apply Article 9 safeguards and a DPIA where required. No such system is authorised by this policy alone. [26]

18 Training monitoring and review

Staff receive induction and regular refresher training appropriate to their role, including children's information, safeguarding disclosure, rights requests, complaints, phishing, AI and immediate breach reporting. Contractors receive equivalent instructions for their access. Managers investigate non-compliance fairly and take action under employment, engagement and safeguarding procedures.

The proprietor reviews compliance at least annually and after a significant incident, system change or legal update. Review access, notices, retention, suppliers, DPIAs, training, deadlines, complaints and lessons from breaches. Read this policy alongside safeguarding, SEND, safer recruitment, records retention, information security, acceptable use, online safety, complaints and image-consent procedures. Record approval and communicate the effective version to all relevant staff.

Appendix A Privacy notice requirements

The original document mixed workforce and pupil notices. Publish separate notices reflecting actual MEPA practice, using the categories and purposes in section 5 and the checks below. This appendix is an implementation specification, not a completed public notice. Do not state that a supplier, pension scheme, regulator or transfer applies unless verified.

Required notice detail	What must be included
Controller and contact	Full legal controller name for each setting; address; data protection contact; DPO contact if appointed; explain any shared controller arrangement.
People and sources	Identify the audience. Explain information provided directly and received from families, education settings, referees, authorities or others, as applicable.
Purposes and legal grounds	Map each actual use to its Article 6 basis; specify legitimate or recognised legitimate interests where used. Explain applicable sensitive-data processing accurately.
Required and optional data	Explain whether provision is statutory, contractual or optional, and the consequences of not providing it. Describe withdrawal of consent.
Sharing and transfers	Actual recipient categories, including processors and independent controllers; overseas countries or relevant arrangements; transfer safeguards and how to obtain them.
Retention	Specific periods or clear criteria and triggers for each relevant category; explain longer legal holds where necessary.
Rights and complaints	Applicable rights, how to exercise them, child and representative arrangements, withdrawal without affecting earlier lawful use, and internal and ICO complaint routes.
Automated processing	Whether significant solely automated decisions exist; where applicable provide meaningful information about the logic, significance, likely consequences and safeguards.
Accessibility and updates	Accessible plain language and child-friendly explanations; issue at the required time, date each version and explain material changes.

Learner and family notices must cover Academy education, College provision and Studios classes as applicable, including waiting lists, attendance, qualifications, SEND, health, welfare, safeguarding, performance licences, fees and images. Workforce notices must cover employees and relevant self-employed staff separately where purposes differ, including recruitment, pay, checks, health, conduct and system use. Provide other notices at the relevant collection points, including visitors, CCTV and websites. [12]

Appendix B Adoption and implementation checklist

The proprietor and data protection lead complete this record before publishing the policy and related notices. Record an owner and completion date against each action. The revised wording does not substitute for these operational checks.

- To complete — Confirm the full legal controller identity and status of each setting, and whether intra-MEPA sharing is within one entity, between independent controllers or jointly controlled.
- To complete — Confirm Emma Finch's role, current address and email; provide a monitored deputy and closure-period incident route.
- To complete — Record the DPO requirement assessment; appoint and publish a compliant DPO where required and notify the ICO. Check the applicable ICO fee registration.
- To complete — Approve the purpose-by-purpose lawful-basis register, Article 9 and Article 10 conditions, appropriate policy documents and legitimate interests assessments.
- To complete — Confirm each setting's section 16LA scope, the September 2026 information sharing duty procedure and the DSL's secure record-transfer arrangements.
- To complete — Approve record-specific retention periods and disposal arrangements; remove the blanket age-25 rule from all related notices and systems.
- To complete — Issue complete, consistent learner, parent, workforce, recruitment, visitor and online notices with verified recipients and transfers.
- To complete — Check processor contracts, education and payroll suppliers, overseas access, transfer safeguards and DPIAs; remove unapproved AI or app access.
- To complete — Test parent portal and integration permissions, separate family access, account removal, encryption, backups and recovery.
- To complete — Implement complaints acknowledgement and investigation logging, rights-request deadlines and the 72-hour breach process, including holiday cover.
- To complete — Check image permissions, marketing opt-outs, cookie settings and any CCTV or biometric use against this policy.
- To complete — Train staff, record approval and effective date, publish the relevant notices and set the August 2027 review.

Appendix C Legislation and guidance sources

Primary sources checked on 10 October 2026. Numbers correspond to references in the policy. Use the current in-force legislation and final guidance rather than consultation drafts; review subsequent changes before the next adoption or material processing change.

1 UK GDPR and Data Protection Act 2018

<https://www.legislation.gov.uk/eur/2016/679/contents>

<https://www.legislation.gov.uk/ukpga/2018/12/contents>

2 DfE Data protection in schools

<https://www.gov.uk/guidance/data-protection-in-schools>

3 Data Use and Access Act 2025 and ICO commencement statement

<https://www.legislation.gov.uk/ukpga/2025/18/contents>

<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/02/statement-on-the-commencement-of-the-data-use-and-access-act-duaa/>

4 DfE The Data Use and Access Act 2025

<https://www.gov.uk/guidance/data-protection-in-schools/the-data-use-and-access-act-2025>

5 DfE Keeping Children Safe in Education 2026

<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

6 DfE Information Sharing Duty September 2026

<https://www.gov.uk/government/publications/information-sharing-to-safeguard-children-and-young-people>

7 DfE Working Together to Safeguard Children 2026

<https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>

8 DfE Role of data protection officers

<https://www.gov.uk/guidance/data-protection-in-schools/role-of-data-protection-officers>

9 DfE What data protection means for schools

<https://www.gov.uk/guidance/data-protection-in-schools/what-data-protection-means-for-schools>

10 DfE Data processing a school is permitted to do

<https://www.gov.uk/guidance/data-protection-in-schools/data-processing-a-school-is-permitted-to-do>

11 ICO Recognised legitimate interest

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/recognised-legitimate-interest/>

12 DfE Data protection policies and procedures

<https://www.gov.uk/guidance/data-protection-in-schools/data-protection-policies-and-procedures>

13 ICO A guide to subject access

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/subject-access-requests/a-guide-to-subject-access/>

14 DfE Procuring educational technology

<https://www.gov.uk/guidance/data-protection-in-schools/procuring-educational-technology-edtech>

15 DfE Record keeping and management

<https://www.gov.uk/guidance/data-protection-in-schools/record-keeping-and-management>

16 DfE Handling other information rights requests

<https://www.gov.uk/guidance/data-protection-in-schools/handling-other-information-rights-requests>

17 ICO What should we consider when responding to a request

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/what-should-we-consider-when-responding-to-a-request/>

18 ICO How to deal with data protection complaints

<https://ico.org.uk/for-organisations/how-to-deal-with-data-protection-complaints/>

19 ICO New complaints law now in force June 2026

<https://cy.ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/06/new-data-protection-complaints-law-now-in-force/>

20 DfE Managing breaches of data

<https://www.gov.uk/guidance/data-protection-in-schools/managing-breaches-of-data>

21 DfE Generative AI and data protection

<https://www.gov.uk/guidance/data-protection-in-schools/generative-artificial-intelligence-ai-and-data-protection-in-schools>

22 ICO Profiling children and automated decisions

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-if-we-want-to-profile-children-or-make-automated-decisions-about-them/>

23 ICO Appropriate safeguards for international transfers

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/appropriate-safeguards/what-are-the-rules-on-appropriate-safeguards/>

24 DfE Taking and using photos videos and CCTV

<https://www.gov.uk/guidance/data-protection-in-schools/taking-and-using-photos-and-videos-and-using-cctv-in-schools>

25 ICO Direct marketing using electronic mail and PECR

<https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-direct-marketing-using-electronic-mail/>

<https://www.legislation.gov.uk/uksi/2003/2426/contents>

26 DfE Protection of children's biometric information

<https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools>

27 DfE Dealing with subject access requests

<https://www.gov.uk/guidance/data-protection-in-schools/dealing-with-subject-access-requests-sars>