

HINDLE'S SCHOOL OF EXCELLENCE LTD

Data Protection and UK GDPR Policy

*Learners, families, staff, volunteers and stakeholders | 2026-27***Our commitment**

Hindle's will use personal information lawfully, fairly, transparently and securely; protect children and vulnerable learners; respect individual rights; and share information responsibly where education, safety, safeguarding or legal duties require it.

Data controller	Hindle's School of Excellence Ltd
Policy owner / data-protection lead	Miss Joanne C. Hindle, Director
Contact	joanne@hindlesschoolofexcellence.co.uk 0161 764 2415
Approved by	Miss Joanne C. Hindle, Director
Approval / effective date	31 August 2026 / 1 September 2026
Policy period	1 September 2026 to 31 August 2027
Next review	1 September 2027
Version / status	2.0 / Approved

Hindle's School of Excellence Ltd
115 Rochdale Road, Bury, BL9 7BA
Registered with the Information Commissioner's Office

1. Purpose and scope

This policy explains how Hindle's School of Excellence Ltd collects, uses, stores, shares, retains and disposes of personal data. It applies to directors, employees, tutors, trainees, volunteers, contractors and others processing personal data on behalf of Hindle's. It covers learner, parent/carer, staff, applicant, volunteer, visitor, commissioner, supplier and other stakeholder information in paper, verbal, visual and electronic form.

2. Legal framework

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Data (Use and Access) Act 2025 and commenced amendments to UK data-protection legislation.
- Privacy and Electronic Communications Regulations 2003 (PECR), where applicable.
- Freedom of Information Act 2000 only where Hindle's is subject to a relevant duty or contractual arrangement.
- Human Rights Act 1998, Equality Act 2010, safeguarding and education legislation, and common-law duties of confidentiality.
- Current Information Commissioner's Office guidance and relevant DfE guidance.

Important correction

Consent is not required for all processing and is often not the most appropriate lawful basis in education, employment or safeguarding. Hindle's will identify and document the correct lawful basis for each purpose. Where consent is relied upon, it must be freely given, specific, informed, unambiguous and capable of withdrawal.

3. Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person.
Special-category data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric identification data, health data, or sex-life/sexual-orientation data.
Criminal-offence data	Personal data relating to criminal allegations, proceedings, convictions or related security measures.

Processing	Any operation on personal data, including collection, recording, viewing, sharing, alteration, storage or deletion.
Controller	The organisation deciding why and how personal data is processed.
Processor	A separate organisation processing personal data on the controller's documented instructions.
Data breach	A security incident causing accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. Data-protection principles

- Lawfulness, fairness and transparency.
- Purpose limitation: use data only for specified, explicit and legitimate purposes unless a lawful compatible use applies.
- Data minimisation: collect and share only what is adequate, relevant and necessary.
- Accuracy: take reasonable steps to keep data correct and current.
- Storage limitation: keep identifiable data only as long as necessary.
- Integrity and confidentiality: use appropriate technical and organisational security.
- Accountability: demonstrate compliance through records, training, contracts, risk assessments and review.

5. Governance and responsibilities

5.1 Director / data-protection lead

- Maintain this policy, privacy notices, the data map/record of processing, retention schedule and breach log.
- Advise on rights requests, lawful bases, information sharing, contracts, DPIAs and security incidents.
- Ensure ICO registration or data-protection fee status remains current where required.
- Coordinate with commissioners, schools, local authorities, professional advisers and the ICO.
- Report material risks and ensure corrective actions are completed.

5.2 Managers and system owners

- Approve access according to role and remove access promptly when duties change or end.

- Select and monitor processors, ensure appropriate contracts, and review system security and data location.
- Build privacy, minimisation, retention and deletion into new processes.
- Ensure staff understand any system-specific procedures.

5.3 All staff, tutors and volunteers

- Use personal data only for authorised work and on a need-to-know basis.
- Follow privacy notices, security procedures, retention rules and lawful management instructions.
- Keep passwords and access devices secure; never share accounts or leave records unattended.
- Check recipients and attachments before sending, and use approved secure channels.
- Report mistakes, suspected breaches, phishing, loss, unauthorised access and rights requests immediately.
- Maintain confidentiality during and after employment, placement or volunteering.

6. Information Hindle's may process

- Identity and contact details, attendance, educational history, assessments, progress, work, qualifications and destinations.
- SEND, disability, health, medication, access arrangements, EHCP information and reasonable adjustments.
- Safeguarding, welfare, behaviour, risk, incidents, allegations and professional involvement.
- Parent/carers communications, consent and emergency contacts.
- Staff, applicant, volunteer, trainee, payroll, tax, pension, absence, performance, training, disciplinary and recruitment information.
- DBS status and other criminal-offence information where lawful and necessary; copies are restricted and retained only where permitted.
- CCTV images and access/security records under the separate CCTV Policy.
- Contracts, commissioning, invoices, payments, insurance, complaints and legal claims.
- Technical information such as account identifiers, device, login, audit and cyber-security records.

7. Privacy information and transparency

Hindle's will provide clear privacy information describing the controller, purposes, categories, lawful bases, recipients, retention, rights, complaint routes and any international transfers or automated decision-making. Privacy information will be accessible and written appropriately for children and other audiences. A material new use will be assessed and communicated before processing unless a lawful exception applies.

8. Lawful bases

Lawful basis	Typical use where applicable
Contract	Delivering agreed tuition/provision, employment or supplier arrangements and steps requested before a contract.
Legal obligation	Tax, employment, health and safety, safeguarding or regulatory records and disclosures required by law.
Vital interests	Protecting life where a person cannot consent or another basis is unavailable.
Public task	Only where Hindle's is exercising a function in the public interest with a clear basis in law; commissioning alone does not automatically make all processing a public task.
Legitimate interests	Necessary proportionate business, safety, safeguarding, service-quality, security or legal interests, after balancing individual rights; recognised legitimate interests may apply where the statutory conditions are met.
Consent	Genuine optional uses where refusal or withdrawal can occur without detriment.

9. Special-category and criminal-offence data

Hindle's will identify both an Article 6 lawful basis and an Article 9 condition for special-category data, such as employment/social-protection law, vital interests, legal claims, substantial public interest with an appropriate policy document, healthcare where applicable, or explicit consent. Criminal-offence data will only be processed under official authority or with a lawful condition and safeguards under the Data Protection Act 2018. Access will be particularly restricted.

10. Children and vulnerable learners

- The best interests, age, understanding, autonomy, safety and vulnerability of children will be considered.
- Privacy information and requests for consent will be age appropriate. Parent/carers involvement depends on the learner's competence, the context and legal duties.

- Safeguarding information may be shared without consent where necessary and lawful; fear of breaching confidentiality must not delay protection.
- Online tools likely to be accessed by children will be assessed for privacy-by-design, default settings, tracking, profiling, transparency and supplier safeguards.
- Children's data will not be used for behavioural advertising or unnecessary profiling.

11. Data minimisation and accuracy

- Collect only information needed for a clear purpose and avoid speculative or excessive notes.
- Record facts accurately, distinguish fact from opinion and identify the source of professional information.
- Provide reasonable opportunities to update contact, health, SEND and emergency information.
- Correct inaccurate data promptly. Where accuracy is disputed, record the challenge and restrict processing where appropriate.
- Do not duplicate sensitive information across systems without a justified need.

12. Approved systems and secure working

- Use approved organisational systems and work accounts. Personal email, personal cloud storage, informal messaging, unapproved apps and personal removable media must not be used for organisational personal data without written approval and safeguards.
- Organisational devices must use supported software, screen locking, encryption where appropriate, malware protection and timely security updates.
- Use strong unique passwords and multi-factor authentication where available. Passwords must be changed after suspected compromise; routine forced changes will follow current security guidance and system requirements.
- Paper records must be kept in secure storage when unattended and transported only where authorised, minimised and protected.
- USB or removable media must be avoided unless necessary and authorised; it must be encrypted, inventoried and securely stored.
- Sensitive conversations and screens must be protected from being overheard or viewed. Printing should be collected immediately.
- Remote and home working must preserve the same confidentiality, access and disposal standards as on-site work.

13. Email, messaging and disclosure controls

1. Confirm the identity and authority of the recipient.

2. Check the address, attachments, distribution list and whether all recipients need the information.
3. Use secure transfer, encryption or password protection proportionate to risk; send passwords by a separate channel.
4. Use BCC appropriately for external group emails.
5. Record significant disclosures and the lawful purpose.
6. If information is sent incorrectly, attempt safe recall/containment and report the breach immediately.

14. Access management

Access will follow least-privilege and role-based principles. Individual accounts must be used. Managers will approve access, review it periodically and remove it promptly when a person leaves or changes role. Audit logs will be enabled and reviewed where appropriate. Shared passwords are prohibited except for formally controlled emergency arrangements.

15. Information sharing and safeguarding

Information may be shared with commissioning schools, local authorities, safeguarding partners, health professionals, examination bodies, regulators, police, courts, insurers and professional advisers where there is a clear lawful purpose. Hindle's will share the minimum necessary, verify the recipient, use secure methods and record significant decisions.

Safeguarding priority

Consent is not a prerequisite for safeguarding information sharing. Staff must refer concerns to the DSL and should not promise absolute confidentiality. The Lead DSL is Joanne C. Hindle; additional/deputy DSLs are Julie Helm, Jade McFarlane and Aman Javed.

16. Processors, suppliers and contracts

- Carry out due diligence covering security, confidentiality, resilience, data location, subcontractors, deletion and support for rights and breaches.
- Put a written Article 28-compliant processor contract in place before processing begins.
- Give documented instructions and permit access only to necessary data.
- Monitor material suppliers and obtain assurance proportionate to risk.
- Ensure data is returned or securely deleted at contract end unless law requires retention.
- Do not assume that a free online service, educational app or AI tool is approved.

17. Artificial intelligence and automated decisions

Staff must not enter identifiable learner, safeguarding, health, staff or commercially confidential information into public or unapproved AI systems. Any proposed AI use involving personal data requires written approval, supplier review, lawful-basis analysis, transparency, security assessment and, where risk is likely to be high, a DPIA. Solely automated decisions producing legal or similarly significant effects will only be used lawfully with required safeguards, including information, challenge, representations and meaningful human intervention.

18. CCTV, images and recordings

- CCTV is governed by the CCTV and Video Surveillance Policy; routine footage is normally retained for up to 31 days unless preserved for an incident or lawful request.
- Cameras will not be used in toilets, changing areas or other spaces with a high expectation of privacy. Audio is off by default.
- Photographs, recordings and publicity uses require a documented lawful basis and clear information; optional promotional use will normally rely on consent.
- Facial recognition, emotion recognition, biometric identification or automated behaviour scoring will not be introduced without a new DPIA, specialist advice, policy amendment and explicit approval.

19. Data protection impact assessments

A DPIA will be completed before processing likely to create a high risk, including large-scale sensitive data, systematic monitoring, innovative technology, significant profiling, biometrics, or combining datasets in unexpected ways. It will describe processing and purpose, assess necessity and proportionality, identify risks to people and document controls. High residual risk will be referred to the ICO where required before processing.

20. International transfers

Personal data will not be transferred or remotely accessed outside the UK unless an adequacy regulation, appropriate safeguards or a permitted exception applies. Hindle's will assess the transfer, document the mechanism and supplementary controls, and explain relevant transfers in privacy information.

21. Individual rights

Right	Hindle's response
-------	-------------------

To be informed	Provide concise, accessible and transparent privacy information.
Access	Confirm processing and provide personal data and required information following reasonable and proportionate searches.
Rectification	Correct incomplete or inaccurate data and notify recipients where required.
Erasure	Delete where the right applies. The right is not absolute and may be refused where data is needed for legal duties, safeguarding, legal claims or other statutory exceptions.
Restriction	Pause or limit relevant processing where the conditions are met.
Data portability	Provide qualifying consent/contract data processed by automated means in a structured, commonly used, machine-readable format.
Object	Consider objections, including to legitimate-interests processing and direct marketing.
Automated decisions	Apply legal safeguards and allow challenge/human intervention where required.
Withdraw consent	Stop consent-based processing prospectively unless another lawful basis applies; withdrawal does not undo prior lawful processing.
Complain	Use Hindle's complaints process and contact the ICO if dissatisfied.

22. Rights-request procedure

7. Forward any verbal or written rights request immediately to the data-protection lead. Staff must not require the words "subject access request".
8. Record the request and acknowledge it. Verify identity proportionately and clarify scope where needed.
9. Search reasonable and proportionate locations, preserve relevant data and consult third parties/commissioners where responsibilities overlap.
10. Review exemptions, third-party information, safeguarding risk and legal restrictions. Redact rather than withhold entire documents where appropriate.
11. Respond without undue delay and normally within one month. The statutory period may be paused while necessary clarification or identity information is awaited under

the current rules, and extended where legally permitted for complex or multiple requests.

12. Keep an audit trail of searches, decisions, disclosure and any refusal or fee. Explain complaint rights.

23. Data retention and secure disposal

Learner information is not automatically deleted when a learner leaves, and individuals do not have an unrestricted right to immediate deletion. Each record category will be retained under an approved schedule reflecting its purpose, statutory requirements, safeguarding needs, contractual obligations, insurance, examination rules and legal limitation periods.

Record category	Retention approach
Safeguarding / child-protection	Follow the safeguarding retention schedule and relevant guidance; preserve for referrals, inquiries or legal claims where required.
Learner education, assessment and provision	Retain for the period needed to evidence delivery, progress, commissioning, transitions, complaints, audit and claims.
Financial, tax and company records	Retain for applicable statutory accounting and tax periods.
Staff and recruitment	Apply employment, safeguarding, pension, payroll and limitation requirements; unsuccessful-applicant records are shorter unless justified.
CCTV	Normally up to 31 days, unless preserved for an incident, complaint, request or legal purpose.
DBS information	Record only permitted status/details; certificate copies and sensitive information are restricted and retained only where lawful.
Temporary working copies	Delete promptly when the approved record is saved and no further purpose remains.

Paper will be cross-cut shredded or placed in confidential-waste arrangements. Electronic data will be securely deleted, accounts closed and storage media securely erased or destroyed. Disposal will be suspended for complaints, investigations, legal holds, safeguarding or rights requests.

24. Personal-data breaches

All actual or suspected breaches must be reported immediately to the data-protection lead, including loss, misdirection, unauthorised access, phishing, malware, excessive disclosure, insecure disposal or unavailable data. Staff must preserve evidence and must not conceal, independently investigate beyond instruction, or contact affected people without authorisation.

13. Contain the incident safely: recall messages, disable links/accounts, recover devices or restrict access where possible.
14. Record what happened, when, systems/data affected, people involved and immediate action.
15. Assess likely consequences, sensitivity, volume, identifiability, vulnerability, security controls and risk to people's rights and freedoms.
16. Notify the ICO without undue delay and, where feasible, within 72 hours of awareness if the breach is likely to risk individuals' rights and freedoms. If notification is late, record reasons.
17. Inform affected individuals without undue delay if high risk is likely, using clear advice on protective action, unless a lawful exception applies.
18. Notify commissioners, insurers, police, safeguarding partners or processors where required.
19. Complete corrective action, lessons learned and breach-log entries. Document the decision even where ICO notification is not required.

Immediate internal reporting

The 72-hour period is an external maximum where notification is required—not an internal reporting target. Staff and volunteers must report a suspected breach to Joanne C. Hindle immediately.

25. Complaints about data use

A person may complain to Hindle's about the way their information is used. The complaint will be acknowledged, investigated by an appropriately independent person where practicable, and answered with the outcome and any action. Records will be kept. The person will be told of their right to complain to the Information Commissioner's Office. This process will reflect the complaints requirements commenced under the Data (Use and Access) Act 2025.

26. Training, confidentiality and monitoring

- All staff and volunteers with data access will receive induction and periodic refresher training appropriate to their role.

- Training will include phishing, secure sharing, children's data, safeguarding, breaches, rights requests, remote working, retention, AI and approved systems.
- Policy acknowledgement and confidentiality obligations will be recorded.
- Compliance may be monitored through access reviews, audits, breach trends, spot checks, supplier reviews and training records.
- Deliberate or negligent misuse may result in disciplinary action, removal of access, contract action, safeguarding referral, regulatory notification or police involvement.

27. Recruitment and DBS information

Safeguarding checks and supervision of volunteers are governed by the Safer Recruitment and Safeguarding policies. Data-protection law does not itself require every person aged 16 or over to undergo a DBS check. Hindle's will obtain the appropriate level of check only where the role and legal eligibility justify it, provide privacy information, restrict access and avoid retaining certificate information longer than permitted.

28. Review and related documents

This policy will be reviewed by 1 September 2027 or earlier following legal or regulatory change, a significant breach, new technology or system, organisational change, complaint findings or updated ICO guidance.

- Privacy notices and consent records.
- Records Retention Schedule and Data Asset / Processing Register.
- Personal Data Breach Procedure.
- Subject Access and Individual Rights Procedure.
- Confidentiality and Information Sharing Policy.
- Safeguarding and Child Protection Policy.
- CCTV and Video Surveillance Policy.
- IT, cyber-security, acceptable-use and remote-working procedures.
- Medication, First Aid, Complaints and Safer Recruitment policies.

Appendix A - Data Sharing Decision Record

Question	Record
What information is proposed for sharing?	
Purpose and expected benefit	
Recipient identity and authority verified	
Article 6 lawful basis	
Article 9 / Schedule 1 condition if needed	
Is consent relevant? If not, why not?	
Minimum data necessary / redactions	
Risks, safeguarding and objections considered	
Secure method and date/time	
Decision-maker and review/follow-up	

Appendix B - Rights Request Log

Received	Requester / identity check	Right and scope	Clarificatio n / clock status	Due date	Outcome / sent	Lead

Appendix C - Personal Data Breach Record

Field	Record
Reference / date and time discovered	
Reporter and contact details	
What happened and how discovered	
Systems, records and locations affected	
Data categories, sensitivity and volume	
Approximate number / type of people affected	
Containment and recovery action	
Processor / commissioner / insurer notified	
Risk assessment and likely consequences	
ICO reportable? Decision, reason and deadline	
Individuals notified? Decision and wording	
Safeguarding / police action	
Root cause and corrective actions	
Closure, review date and sign-off	

Appendix D - Staff Data-Handling Checklist

Before collecting

Define the purpose, lawful basis, minimum fields, privacy information, retention and approved system.

Before sharing

Verify identity and authority, check necessity and accuracy, minimise/redact, use a secure method and record significant decisions.

Before working remotely

Use an approved account/device, protect screens and conversations, avoid local copies, and secure any authorised papers in transit and at home.

If something goes wrong

Contain only where safe, preserve evidence and report immediately to Joanne C. Hindle. Do not wait to see whether harm occurs.

When data is no longer needed

Follow the retention schedule, check for holds or active requests, and use confidential destruction or secure electronic deletion.