

HINDLE'S

SCHOOL OF EXCELLENCE LTD

CONFIDENTIALITY AND INFORMATION-SHARING POLICY

Protecting privacy while sharing information lawfully to keep children safe

Setting	Hindle's School of Excellence Ltd
Address	115 Rochdale Road, Bury, BL9 7BA
Policy owner	Director / Data Protection Lead
Safeguarding lead	Designated Safeguarding Lead
Effective date	1 September 2026
Next review	September 2027, or sooner if requirements change
Applies to	Staff, tutors, trainees, volunteers, contractors and governors/advisers
Key rule Share only what is necessary, with authorised people, for a clear lawful purpose. Never allow confidentiality concerns to delay action needed to protect a child.	

1. Purpose and scope

Hindle's School of Excellence Ltd handles personal and special-category information about children, young people, parents, carers, staff, applicants, commissioners and other service users. This policy sets expectations for confidentiality, secure record handling and lawful information sharing in tuition, alternative provision, childcare, online learning, home tuition and off-site activities.

This policy supports, but does not replace, the Data Protection Policy, privacy notices, Records Retention Schedule, Data Breach Procedure, Safeguarding and Child Protection Policy, Online Safety Policy, Staff Code of Conduct, Bring Your Own Device arrangements and contractual information-sharing agreements.

2. Legal and guidance framework

- UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and Data (Use and Access) Act 2025;
- Human Rights Act 1998 and common-law duty of confidence;
- Children Acts 1989 and 2004, Education Act 2002 and relevant safeguarding duties;
- Keeping Children Safe in Education 2026 and Working Together to Safeguard Children 2026;
- DfE Information Sharing: advice for practitioners providing safeguarding services (May 2024); and
- ICO Data Sharing Code of Practice and guidance on sharing data to safeguard children.

3. Key definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person.
Special-category data	Data requiring extra protection, including health, ethnicity, religion, sexual orientation and biometric data used for identification.
Criminal-offence data	Information about alleged or proven offences, proceedings or convictions.
Confidential information	Information given or held in circumstances where privacy is reasonably expected; it may include information that is not personal data.
Processing	Any operation involving data, including collecting, viewing, recording, sharing, storing, altering and destroying it.
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 information only for specified, legitimate purposes;
- data minimisation – collect and share only what is adequate, relevant and necessary;

- accuracy – keep records correct and update or annotate them when needed;
- storage limitation – retain information only for as long as required;
- integrity and confidentiality – use appropriate technical and organisational security; and
- accountability – record decisions and demonstrate compliance.

5. Roles and responsibilities

- The Director is responsible for organisational compliance, resources, contracts, privacy notices and oversight of breaches.
- The Data Protection Lead advises on lawful processing, rights requests, data protection impact assessments, retention and breach reporting.
- The DSL decides and records safeguarding information sharing, consulting the Data Protection Lead where this can be done without delaying protection.
- Managers ensure access is role-based, staff are trained and local working practices comply with this policy.
- Every worker must protect information, access only what they need, use approved systems, report incidents immediately and maintain confidentiality after their role ends.

6. Lawful processing and consent

Hindle's will identify and document an Article 6 lawful basis for processing personal data and, where special-category or criminal-offence data is involved, an additional condition under the Data Protection Act 2018. Depending on the purpose, relevant bases may include legal obligation, public task, contract, vital interests, legitimate interests or consent.

Important correction Consent is not the only lawful basis and is often not the appropriate basis for education, safeguarding, employment or contractual administration. Consent must not be presented as compulsory where the activity will proceed under another lawful basis.

Where consent is relied upon, it must be freely given, specific, informed, unambiguous, recorded and capable of withdrawal. Withdrawal will not make earlier lawful processing unlawful. Children's competence, best interests, age-appropriate information and parental responsibility will be considered.

7. Confidentiality and safeguarding

Confidentiality is not absolute. Staff must never promise a child, parent or colleague that information will be kept secret. They should explain that information will be shared only with people who need it to provide support, fulfil duties or protect someone from harm.

Safeguarding rule You do not need consent to share a child's personal information for safeguarding purposes where there is a lawful basis. Data-protection law allows proportionate sharing to identify and protect children at risk. It may be more harmful not to share.

Where safe and appropriate, the child and/or family should be told what will be shared, with whom and why. They should not be informed first where this could increase risk, prejudice an investigation, lead to evidence being destroyed, place another person at risk or otherwise undermine safeguarding action. The DSL will record the decision and rationale.

8. Seven information-sharing checks

1. Is there a clear purpose and a need to share?
2. Is there a lawful basis and, if relevant, a special-category or criminal-data condition?
3. Can the person be informed safely, and are their wishes relevant even where consent is not required?
4. Is the information accurate, relevant, necessary and limited to what the recipient needs?
5. Is the recipient's identity, authority and secure contact route verified?
6. Is sharing necessary, proportionate, timely and in the child's best interests?
7. Has the decision, information shared, recipient, date, purpose and any advice obtained been recorded?

If in doubt, staff should consult the DSL or Data Protection Lead. Doubt must not delay emergency action or a safeguarding referral.

9. When information may or must be shared without consent

- to safeguard a child or adult at risk, including perceived risk of harm, neglect, exploitation, self-harm or suicide;
- to prevent or detect crime, protect someone's vital interests or respond to a serious threat;
- to comply with a court order, statutory duty, police power, regulator, inspector or lawful professional request;
- to transfer safeguarding information to a new education setting or coordinate multi-agency support;
- to respond to allegations about adults working with children, LADO, MASH or police processes; or
- where another lawful basis and condition applies and sharing is necessary and proportionate.

A disclosure that a crime may have occurred does not automatically justify sharing everything with anyone. The DSL, Director or Data Protection Lead will consider the purpose, seriousness, safeguarding implications, legal power and minimum necessary information. In an emergency call 999.

10. Receiving requests for information

Unsolicited requests must be treated cautiously. Staff must not confirm whether a person is a learner or service user, or disclose attendance, contact details, location, health, family or safeguarding information, until the requester's identity, authority, purpose and secure contact route have been verified.

- Refer police, solicitor, court, local-authority, commissioner, media and regulator requests to the Director, DSL or Data Protection Lead as appropriate.
- Do not rely solely on caller identification, an email signature or information the requester already knows.
- Record the request and decision. Preserve relevant records if litigation, an investigation or a statutory inquiry is reasonably anticipated.
- Urgent safeguarding requests should be verified and responded to without avoidable delay.

11. Recording on CPOMS and other approved systems

CPOMS and other approved management systems may be used only by authorised staff for defined purposes. Access will be role-based, reviewed regularly and removed promptly when no longer required. Staff must use their own account, strong authentication and factual, professional language. Records must distinguish fact, observation, disclosure, opinion and action taken.

- Do not include irrelevant personal opinions, insulting language or excessive detail.
- Do not share passwords or leave a signed-in device unattended.
- Do not download, print, photograph, screenshot or export records unless authorised and necessary.
- Audit logs and access records may be monitored for security, safeguarding and compliance.
- Corrections should preserve the audit trail; safeguarding records must not be silently overwritten or deleted.

12. Spreadsheets, email and electronic transfer

Spreadsheets and email are higher-risk where they contain personal data. They may be used only where approved and necessary. Password protection alone is not a complete security measure.

- Use an approved organisational account and the minimum required data; use a unique identifier instead of a name where practical.
- Check recipients and attachments before sending. Use BCC for unrelated external recipients where appropriate.
- Use approved encryption, secure portals or access-controlled links for sensitive information. Send passwords through a separate channel.
- Set expiry dates and disable downloading where the platform permits and the risk justifies it.
- Do not auto-forward work email to personal accounts or upload data to personal cloud storage, messaging apps or AI services.
- Delete working copies promptly when no longer needed and retain the authoritative record in the approved system.

13. Devices, remote work and home tuition

- Use company-managed devices wherever possible. Personal devices require prior written approval and must meet security requirements.
- Use screen locks, supported software, encryption, multi-factor authentication and secure networks. Do not use public shared computers.
- Position screens and conduct calls so others cannot see or overhear confidential information.
- Do not leave devices or records visible in vehicles. Report loss, theft or suspected compromise immediately.
- Do not allow family members or learners to use a work device containing organisational information.
- Keep local downloads to an absolute minimum and remove them securely when the task is complete.

14. Paper records and off-site working

Paper records will be kept in locked storage within secure premises and accessed only by authorised staff. Visitors must not be left unaccompanied where records are accessible. Clear-desk practices apply when rooms are unattended.

- Original records should not leave the setting unless necessary and authorised.
- For trips, emergencies or home tuition, take only the minimum documents required and use a secure, closed bag. Maintain possession or approved locked storage.
- Paper records must not be left overnight in a vehicle. Taking records to a private home requires manager approval and secure storage inaccessible to household members.
- Return records to the setting as soon as practicable and record any temporary removal where required.
- Destroy confidential paper using cross-cut shredding or an approved confidential-waste service; never place it in ordinary recycling or waste.

15. Photographs, video, publicity and training

Identifiable photographs, recordings and case studies are personal data. Hindle's will identify a lawful basis, provide appropriate privacy information and obtain consent where consent is the chosen basis. Publicity consent will be separate from essential educational services and refusal will not cause detriment. Consent will specify the intended channels and can be withdrawn for future use, although material already lawfully published may not always be fully retrievable.

Training and supervision examples should be anonymised or pseudonymised wherever possible. True anonymisation means a person is no longer reasonably identifiable. Changing only a name is usually pseudonymisation and remains personal data.

16. Data analysis, marketing and research

Data used for planning, quality assurance, supervision and reporting will be aggregated or anonymised wherever possible. If individuals remain identifiable, the processing remains subject to data-protection law. Personal data will not be sold. Direct marketing will comply with UK GDPR, the Privacy and Electronic Communications Regulations and children's best interests. Profiling or novel technology involving higher risk will be assessed through a data protection impact assessment where required.

17. Record retention and secure destruction

Records will be retained according to Hindle's approved Records Retention Schedule, applicable law, safeguarding guidance, funding and contractual requirements, limitation periods and operational need. They will not be kept indefinitely "just in case". A legal hold, safeguarding need, complaint or investigation may temporarily suspend routine destruction.

At the end of the retention period, paper and electronic records will be securely destroyed so they cannot be reconstructed. Disposal will include copies, exports, backups where practicable, local downloads and removable media. Destruction decisions will be documented where required.

18. Individual rights and access to records

Individuals may have rights to be informed, access their personal data, request rectification, erasure or restriction, object to processing, data portability and safeguards around automated decisions. Rights depend on the lawful basis and exemptions. Requests must be forwarded immediately to the Data Protection Lead and should normally be answered within one month, subject to lawful extensions.

Parents do not automatically have an unrestricted right to all information about a child. Hindle's will consider the child's competence and rights, parental responsibility, court orders, safeguarding risk, confidentiality owed to others and applicable education-record rules. Third-party information will be redacted where necessary and lawful.

19. Personal-data breaches

Report immediately Any loss, misdirection, unauthorised access, disclosure, cyber incident, missing paper record or suspected compromise must be reported to the Director/Data Protection Lead at once. Do not wait to confirm harm and do not attempt to conceal or investigate alone.

8. Take safe immediate action, such as recalling an email, securing an account, retrieving a document or disconnecting an affected device, without destroying evidence.
9. Tell the Data Protection Lead what happened, when, whose data is involved, likely recipients, actions taken and any continuing risk.
10. Preserve evidence and follow instructions. Do not contact affected people or regulators unless authorised.
11. The Data Protection Lead will assess risk, document the decision and, where required, notify the ICO within 72 hours of becoming aware and notify affected individuals without undue delay where the risk is high.
12. Lessons and corrective actions will be recorded. Disciplinary action may apply where policy was knowingly or recklessly breached, but prompt reporting will be encouraged.

20. Confidentiality exceptions and protected disclosures

Information may be disclosed where there is a lawful and proportionate basis, including safeguarding, serious risk to self or others, legal duties, court orders, regulatory inspection, crime prevention or detection, terrorism concerns, public-interest disclosures and defence of legal claims. The minimum necessary information will be shared with an appropriate recipient. Staff making a protected whistleblowing disclosure should follow the Whistleblowing Policy.

21. Training, audit and non-compliance

All workers will receive confidentiality, safeguarding, cyber-security and data-protection training at induction and regular updates thereafter. Compliance may be audited through access logs, record sampling, device checks, retention reviews and supervision. Failure to follow this policy may result in restricted access, retraining, disciplinary action, termination of contract or referral to regulators, police or professional bodies, depending on seriousness.

22. Review

This policy will be reviewed annually and sooner following a significant breach, inspection finding, change in legislation or guidance, new system, high-risk processing activity or organisational change.

23. Key sources

- **DfE information-sharing advice for safeguarding practitioners** – <https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice>
- **Keeping Children Safe in Education 2026** – <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>
- **Working Together to Safeguard Children 2026** – <https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>
- **ICO 10-step guide to sharing information to safeguard children** – <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/>
- **DfE data-protection guidance for schools** – <https://www.gov.uk/guidance/data-protection-in-schools>

Approval and review record

Version	Approved by	Effective date	Next review
2.0	Joanne C. Hindle, Director	1 September 2026	September 2027
Interim review / amendment:			
Signature:			

Staff confidentiality declaration

I confirm that I have received, read and understood the Hindle's School of Excellence Ltd Confidentiality and Information-Sharing Policy. I understand that:

- my duty of confidentiality continues after my employment, placement or volunteering ends;
- I must access and share information only for authorised work purposes and on a need-to-know basis;
- I must use approved systems and must not use personal email, cloud storage, messaging, removable media or AI tools for organisational personal data without written approval;
- I must report safeguarding concerns and suspected data breaches immediately;
- I must not promise secrecy and must not allow data-protection concerns to delay necessary safeguarding action; and
- breaches may lead to disciplinary, contractual, regulatory or legal action.

Name: _____

Role: _____

Signature: _____

Date: _____

Please sign and return this declaration to Joanne C. Hindle, Hindle's School of Excellence Ltd, 115 Rochdale Road, Bury, BL9 7BA.