HYLTON CASTLE PRIMARY SCHOOL

DATA PROTECTION POLICY

Link governors: Caroline Comer
Policy written by: Emma Olsen
Date ratified by governors: February 2026
Review date: February 2027

Introduction

This Data Protection Policy has been produced to ensure compliance with the Data Protection Act 2018 (the DPA 2018) the General Data Protection Regulation (GDPR) and all associated legislations.

The DPA 2018 gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

In light of the enactment of the Data (Use and Access) Act 2025 (DUAA), this policy has been updated to reflect the amended UK GDPR and Data Protection Act 2018 regime, preserving core privacy protections while enabling responsible data use under DUAA's new flexibilities

Hylton Castle Primary School is registered with the information commissioner's officer as the data controller for the purposes for the personal data its process about individuals.

The school has an appointed Data Protection Officer to:

- Inform and advise the business and its employees about their obligations to comply with the GDPR and other data protection laws.

- Monitor the business's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits and providing the required training to staff members.

- The DPO reports to the highest level of management at the school, which is the School Business Manager.

- Our data protection officer is provided by ADNS Group and can be contacted at the following address:

Scott Thornhill
5 Eggleston Court, Riverside Park
Middlesbrough
TS2 1RU
Tel No: 01642 248750
Email: compliance@adnsgroup.com

Purpose

This policy is a requirement of the DPA 2018, DUAA 2025 and the GDPR. The policy outlines our overall approach to its responsibilities and legal obligations as the 'Data controller' under all legislation.

Scope

This policy applies to all employees (including temporary, casual or agency staff) governors, contracts and consultants working for or on behalf of the school. It also applies to any service providers that we contract with who process personal information on behalf of the school.

This policy also covers any staff who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research or as part of a professional practise activities. If this occurs, it is the responsibility of the company to ensure the data is processed In accordance with the current legislation and that students and staff are advised about their responsibilities.

Data covered by the policy

A detailed description of this definition is available from the ICO, however briefly, personal data is information relating to an individual where the structure of the data allows information to be accessed i.e., as part of a relevant filing system. This includes data held manually and electronically and data compiled, stored, or otherwise processed by us or by a third party on its behalf.

Special category data is personal data consisting of information relating to:

- Racial or ethnic origin
- Political opinions, religious beliefs, or other beliefs of a similar nature
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health or condition
- Sexual life or sexual orientation

The six data protection principles

The DPA 2018 requires the business, including staff, governors and other individual who process personal information on behalf of the school, we must comply with the six data protection principles.

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner. incompatible with that purpose.
- Be limited to only what is required for the purposes for which it is being collected.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for the purpose.
- Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction, or damage.

All new members of staff will be required to complete a mandatory information governance module as part of their induction and existing staff will be requested to undertake refresher training on a regular/annual basis.

Employees within the School are expected to:

- Familiarise themselves and comply with the six data protection principles
- Ensure any possession of personal data is accurate and up to date
- Ensure their own personal information is accurate and up to date
- Keep personal data for no longer than is necessary.
- Ensure that any personal data they process is secure and in compliance with the businesss information related policies and strategies.
- Acknowledge data subjects' rights (e.g. right of access to all their personal data held by the school under the DPA 2018, and comply with access to records.
- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern the business.
- Obtain consent with collecting, sharing, or disclosing personal data.

Employees can contact the DPO at compliance@adnsgroup.com if they require advice or guidance, need to report data protection breach, or have any concerns relating to the processing of personal data under the DPA 2018.

Records Management and Responsibilities

Hylton Castle Primary School must manage its records and record-keeping systems in compliance with applicable regulations, including the Data (Use and Access) Act 2025. This legislation updates UK GDPR, Data Protection Act 2018, and PECR.

The Data Protection Officer (DPO), School Business Manager & Head Teacher hold overall responsibility for this policy. School Business Manager serves as the accountable champion: overseeing policy and strategy, ensuring resources are allocated, and triggering remediation when issues arise. They'll provide guidance on records management best practices, ensuring information is accurate, readily retrievable, and managed securely and promptly. Compliance will be monitored through an annual review to verify secure storage and appropriate access. They'll also advocate for resources and training under the enhanced requirements introduced by the 2025 Act.

More information can be found at the school retention schedule.

Obtaining, disclosing, and sharing

Only personal data that is necessary for a specific business reason should be obtained.

The school will be notified of how information will be processed and is responsible for obtaining the permissions from the pupils.

Upon acceptance of employment, our members of staff also consent to the processing and storage of their data.

Data must be collected and stored in a secure manner. Personal information must not be disclosed to a third-party organisation without prior consent of the individual concerned unless the disclosure is legally

required or permitted. This also includes information that would confirm whether an individual is or has been an applicant, student, or employee of school.

Hylton Castle Primary School may have a duty to disclose personal information to comply with legal or statutory obligation. The DPA 2018 may permit the business to share data without consent or without informing individuals in accordance with the right to be informed:

1. With the police and law enforcement bodies where it is considered necessary for the prevention and detection of crime.
2. Where the information may be necessary under enactment, for the purposes of legal proceedings and or for exercising of defending legal rights.
3. Where the processing is necessary because it is a task carried out for in the public interest, for example sharing information with the local authority, for example safeguarding and child protection.

All requests from third party organisations seeking access, to personal data held by us should be directed to the school office and/or the Data Protection Officer at compliance@adnsgroup.com. We will keep a record of all requests received from third party organisations. This information may be requested by the DPO or the information commissioner at any time to comply and actively evidence compliance, with data subject rights.

Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purview and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the DPA 2018.

Retention, security, and disposal

Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up to date. If an employee, student, or applicant is dissatisfied with the accuracy of their personal data, then they must inform the School Business Manager

Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with data protection principles of the DPA 2018, personal information shall be collected and retained only for business, regulatory or legal purposes.

In accordance with the provisions of the DPA 2018, all staff whose work involves processing personal data, whether in electronic or paper format must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of or damage to personal data. Staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

All departments should ensure that data is destroyed in accordance with the retention schedule when its no longer required. Personal data in paper format must be shredded. Personal data in electronic format should be deleted. Hardware should be appropriately degaussed in compliance with IT service provider contract to ensure the data held on the external device is screened, reviewed before being degaussed and securely destroyed.

Transferring personal data

Any transfer of personal data must be done securely in line with the school's information security and acceptable user agreement. Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with a password provided to the recipient by separate means such as via telephone.

Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly, and care is taken when using reply all or forwarding or copying others into emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

Personal email accounts should not be used to send or receive personal data for work purpose.

Data subjects (subject access requests)

Under the Data Protection Act 2018 and the Data Use and Access Act (DUAA), individuals have the following rights:

- Access to personal information processed by the school.
- Object to processing of personal data that is likely to cause, or is causing, damage or distress.
- Prevent processing for direct marketing.
- Object to decisions being taken solely by automated means.
- In certain circumstances, have inaccurate or incomplete personal data rectified, blocked, restricted, erased or destroyed.

Individuals can make a 'subject access request' (SAR) to any member of school staff, verbally or in writing, to request access to personal information the school holds about them, subject to any exemptions or restrictions that may apply. The school shall use its discretion under the DPA 2018 and DUAA to encourage informal access at a local level to a data subject's personal information, but the school's formal procedure for processing SARs must be followed to comply with legislation.

Any individual who wishes to exercise their right of access can do so verbally or in writing. The school may not charge a fee. Information will only be released upon receipt of the completed SAR form, along with proof of identity or proof of authorisation where requests are made on behalf of a data subject by a third party.

The requested information will be provided within the statutory timescale of one month from receipt of the request. Where clarification is required, the statutory timeframe will be paused ("stop the clock") until the requested information is provided. In cases of complex or multiple requests, the school may extend the timeframe by up to two additional months, notifying the individual within the original one-month period and explaining the reason for the extension.

Under DUAA, the school will conduct reasonable and proportionate searches to locate requested information. The school will not be required to search every system or archive where this would be disproportionate. Information subject to legal privilege or other statutory exemptions will not be disclosed. The school must maintain a formal internal complaints process for SARs.

Complaints can be made via an online form that can be requested by the school. All complaints will be acknowledged within 30 days, investigated transparently, and updates provided throughout. Individuals retain the right to escalate complaints to the Information Commissioner's Office (ICO) if dissatisfied.

Reporting a data security breach

We are legally required to notify the ICO of any data breach within 72 hours, in accordance with the Data Protection Act and the Data (Use and Access) Act 2025. All breaches—regardless of size—must be reported and managed in line with the company's Data Breach and Data Protection policies. Failure to comply may result in fines or enforcement action by the ICO. Where appropriate, additional training will be provided to employees involved, based on severity and recurrence.

All breaches, whether minor or significant, must be reported immediately to the Data Protection Officer (DPO) at ADNS Group (contact: 01642 248750). The DPO will investigate the incident within 24 hours and record it in the breach register, even if no harm occurred.

Following the initial investigation, the DPO will assess the severity of the breach and inform senior management. If necessary, legal advice will be sought. This assessment will be completed within 24 hours of breach awareness.

The DPO and business managers will develop a recovery plan to minimize risks. Interviews with involved individuals will identify root causes and corrective measures within 24 hours of the assessment.

If the breach poses a risk to individuals' rights and freedoms, the ICO will be notified within 72 hours. Affected individuals will also be informed within this timeframe. Notifications will include:

- Details of the breach (what happened, how, and when it was discovered)
- Individuals affected
- Actions taken in response
- Contact details for follow-up

Affected individuals will receive clear and transparent communication. Depending on severity, relevant third parties—such as employees, sponsors, or insurers, will also be notified within five days of breach awareness.