HYLTON CASTLE PRIMARY SCHOOL

DATA PROTECTION POLICY

Link governors: Caroline Comer

Policy written by: Lisa Wood

Date ratified by governors: December 2024

Review date: October 2025

Wood

Table of Contents

Introduction

Hylton Castle Primary school's 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.

The school is registered with the information commissioners' officer as the data controller for the purposes for the personal data its process about individuals.

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 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 school to ensure the data is processed in accordance with the DPA 2018 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 the trust 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.
- Biometric data.

The six Data Protection principles

The DPA 2018 requires the trust, including staff, governors and other individual who process personal information on behalf of the trust, 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.
- Be limited to only what is required for the purposes for which it is being collected.
- Be accurate and kept up to date.
- Not to be kept for longer than is necessary for those purpose.
- Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Responsibilities

Hylton Castle has an appointed Data Protection Officer to:

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

- Monitor the school'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 (NAME/ROLE HERE)

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

  Jessica O'Hara
  5 Eggleston Court, Riverside Park
  Middlesbrough
  TS2 1RU
  Tel No: 03003033793
  Email: compliance@adnsgroup.com

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 trusts information related policies and strategies.
- Acknowledge data subjects' rights (i.e. 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 school.
- Obtain consent with collecting, sharing or disclosing personal data.

- 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.

Obtaining, disclosing, and sharing

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

Parents are informed about how their child's data will be processed when they sign the permissions from upon registration.

Upon the acceptance of employment within the school 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 individuals is or has been applicant, student or employee of the school.

The school may have a duty to disclose personal information to comply with legal or statutory obligation. The DPA 2018 may permit the school 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 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 the school should be directed to the Headteacher and the Data Protection Officer at compliance@adnsgroup.com. The school 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 will 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 or their personal data, then they must inform the head teacher.

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 who's 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 should be shredded. Personal data in electronic format should be deleted. Hardware should be appropriately degaussed in compliance with your 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 online safety policy 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 send 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 DPA 2018, individuals (staff, pupils parents and governors and students etc) 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 by automated means.
- In certain circumstances have inaccurate or incomplete personal data rectified, blocked, restricted, erased or destroyed.
- Claim compensation for damages caused by a breach of the Data Protection regulations.

Individuals can make a 'subject access request' 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 to encourage informal access at a local level to a data subjects' 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 to encourage informal access at a local event to a data subjects' personal information, but the schools' formal procedure for the processing of subject access requests must be followed to comply with the DPA 2018.

Any individual who wishes to exercise their right of access can do so verbally or in writing. There is no legal requirement to ask the requester to keep the schools subject access request form., but it may ask the requester to do so. A copy of the schools' subject access request form is available in appendix one of this document or by contacting the school office:

HYLTON CASTLE PRIMARY SCHOOL

CAITHNESS ROAD

HYLTON CASTLE

SUNDERLAND

TYNE & WEAR.

SR5 3RE

Tel No. (0191) 562 3299

Email: info@hyltoncastleprimary.org.uk

The school may not charge a fee. It will only release any information upon receipt of the completed subject access request 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 1 month from receipt of the completed form.

For details of your other rights please see your information, your rights in appendix two of this document.

Reporting a data security breach

It is important that the trust responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on the trust systems, unauthorised use of personal

data, accidental loss, or equipment failure. Any data breach should be reported to the head teacher – Mrs Wood. The lead investigation officer will then inform the Data Protection Officer, and if it relates to an IT incident (including information security) in certain circumstances it should also be reported to your IT provider.

This policy applies to all staff and pupils and contractors within the school. This includes teaching students, temporary, casual, agency staff, suppliers and data processors working for or on behalf of the school.

Any breach will be investigated in line with the procedures within the Data breach policy. In accordance with that policy, the school will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

If a breach occurs or is discovered outside normal working hours, it must be reported to the school soon as practicable. Note: the school must report data breaches that result or are likely to result in high-risk rights and freedoms of individuals to the information commissioner with the undue delay and in any event within 72 hours.

The school will complete a data breach report that shall include facts relating to the breach, its effect on individuals, the action taken by the trust to mitigate any risk. The report must include full and accurate details of the incident, when the breach occurred (dates and times) who is reporting it, if the data relates to people, the nature of the information and how many people are involved.

CCTV System

The school has operational CCTV with cameras located externally within the building. Images captured by the CCTV are necessary for the prevention and detection of crime and site security. The school has a CCTV policy governing the details, the purposes, use and management of the CCTV system. Hylton Castle have implemented procedures that must be followed to ensure that the trust complies with data protection, human rights and statutory codes of practise published by the information commissioner.

All personal data captured on the CCTV system will only be processed in accordance with the Data Protection Act 2018, the General Protection Regulation (GDPR) and any subsequent data protection legislation and to the Freedom of Information act 2000, the Protection of Freedoms act 2012 and the Human Rights Act 1998.

Although not a relevant authority, the school will also have due regard to the surveillance camera code of practise, issued under the protection of Freedoms Act 2012 and the 12 guiding principles contained therein.

Appendix one- Data Subject Access request form

PERSONAL DETAILS

We need your personal details to find the personal data that we hold about you and your child.

We will keep this form on file for up to two years after we reply to your request. We may transfer some of the information you provide to a computerised database to help us monitor and improve our performance. After two years we will destroy this form and delete identifying details form our database.

Your Name _____

Child/Children's Name/s _____

_____

Only people who have parental responsibility or the child themselves if over, the age of 13 can access data about them

Please confirm your relationship to the child

_____

Address _____

_____**Post code** _____

Telephone _____

Date of birth if requesting your data _____

Date of birth of your child/children if requesting their data _____

If you have lived at this address for less than two years

Previous Address _____

_____**Postcode** _____

Please provide any additional information you think we may need to find your personal data i.e the dates you/your child attended our school, if not a current pupil.

<u>Data Subject Declaration</u>

I wish to access personal data that Hylton Castle Primary School holds. I understand that the school will need to confirm my identity and my relationship to the child if I am making a request to access a child's data. I understand that the school/academy may need to contact me to obtain more information from me to find the data that I have requested.

The 30 day reply period begins once I have provided all the information the school needs.

Please send me all of the information I am entitled to under the Data Protection Act 2018.

Signed----------Date ----------

Agent's Declaration

If you are **Not** the data subject but have authority to act on his or her behalf, you must complete this declaration.

I understand the school may need to contact me to confirm my identity. I understand that the school may need more information from me to find the personal data that I have requested. The 30 day reply period begins once I have provided all the information the school/academy needs.

I confirm that I act on behalf of the Data Subject named overleaf and I have shown to the school proof of my authority to do so.

Signed **Date...**.....

Please return this form to:

Miss Campbell

Hylton Castle Primary School

Caithness Road

Hylton Castle

Sunderland

SR5 3RE

info@hyltoncastleprimary.org.uk

If you would like help completing this form, please contact Miss Campbell.

Right to be informed (what we must tell you)

When we collect personal data from you, at the time we collect t we will.

- Provide you with our contact details
- Provide you with the contact details of our Data Protection Officer.

Tell you what we will do with your personal data, including sharing it with third parties and the legal basis for the processing. We do this by way of a privacy notice. In the unlikely event we need to transfer your personal data to a country that is not covered by the GDPR, we will let you know whether the European Commission has decided regarding the adequacy of that the countries data protection practises. In the unlikely event we need to transfer your personal data to an international organisation we will provide you with details of the safeguards that have been put in place to keep your personal data secure.

Tell you how long we will keep your personal data and what your rights are in relation to that data. These may include the right to have any errors in your personal data corrected, the right to have your personal data erased, the right to stop us processing your personal data and the right to object to us processing your personal data. Please note not all these rights apply in all situations. We will provide you with specific information on which rights at the point we collect your personal data.

Inform you of any automated decision making, including profiling and what the consequences of that decision might be. We will also provide you with the contact details of a person who you can contact for an explanation of the decision. You will be able to inform that person of your point of view and ask them to revisit the decision considering what you have told them.

Where we have asked for your consent to process personal data, we will also provide you with information on your right to withdraw consent at any time. We will tell you if providing tour personal data is statutory or contractual and where you are obliged to provide your personal data. We will also tell you the consequences of you not providing the data.

If we would like to process your personal data for a reason other than that for which we collected it, we will contact you before doing so. We will also provide you with any further information necessary to ensure the way we process your personal data is fair and transparent and inform you or your right to make a complaint to the Information Commissioners Office (ICO). We will usually provide this information in writing. This is known as a privacy notice. We may provide this information in combination with standardised icons to give a clear visual

overview of the intended processing. In cases where you have already received this information, we may not provide it to you.

When we have received your personal data from someone other than you…

In addition to the above information, we will let you know the categories of personal data, for example whether we have received your name, an identification number, location data, an online identifier, or information about your physical, psychological, genetic, mental, economic, cultural, or social identity. We will also tell you who provided us with the information, including whether it came from a publicly accessible source.

We will provide this information to you in a reasonable period depending on the circumstances of the case and in all cases at the latest within one month of the date we received your personal data. If we intend to use your personal data to contact you, we will provide this information at the point of first contact, at the latest. If we intend to disclose the information to a third party, we will provide this information at the point we first disclose your personal data, at the latest.

There maybe some circumstances in which we could not provide you with this information, i.e. where providing this information proves impossible or would involve disproportionate effort, where obtaining or disclosing your information is laid down in law or where the personal data must remain confidential subject to an obligation of professional secrecy regulated by law, including a statutory obligation of secrecy.

Wherever we received your personal data from, the GDPR allows us to use it for archiving in the public interest, for scientific or historical research or for statistical purposes. You do, however have the right to object to such processing. If we do use your personal data for any of these reasons, we must keep it safe in accordance with the GDPR and the Data Protection Act 2018.

Right of access (to your personal data)

You can request a copy of your personal data by writing to your executive head teacher Mrs Wood by email Info@hyltoncastleprimary.org.uk The purpose of being able to access your personal data is so you can be aware of and verify the lawfulness of processing.

On making a request we will need to confirm your identity and whether we hold your personal data. Where we do hold your personal data, we will usually provide you with a copy. Where we hold a lot of information about you, we may ask you to specify what information you would like us to provide. In addition to providing, you with a copy of your personal data we will provide the following information:

1. The purposes of the processing.
2. The categories of personal data;
3. Who we have or will disclose your personal data to, recipients in countries not covered by the GDPR or international organisations.
4. How long we will store your personal data for.
5. Whether you have the right to request your personal data be corrected if it is inaccurate.
6. Whether you have the right to request your personal data be erased.
7. Whether you have the right to request that we stop processing your data or to object to us processing your personal data.

8. Your right to make a complaint to the ICO.
9. Where we received your personal data from, if we did not receive it from you;
10. The existence of automated decision-making, including profiling, along with some meaningful information about the logic involved and the significance and possible consequences of such processing.
11. In the unlikely event we have transferred your personal data to a country that is not covered by the GDPR, we will let you know whether the European Commission has decided regarding the adequacy of that country's data protection practices. Where the European Commission has not decided regarding the adequacy of that countries data protection practices, we will provide you with details of the safeguards that have been put in place to keep your personal data secure; and
12. In the unlikely event we have transferred your personal data to an international organisation, we will provide you with details of the safeguards that have been put in place to keep your personal data secure.

We may not be able to provide you with a copy of your personal data were doing so would adversely affect the right and freedoms of others. For further information about your right of access, please contact our Data Protection Officer.

Right to rectification

If we hold inaccurate personal data about you, you have the right to have it corrected.

Where we have corrected your personal data, we will notify any third parties we have disclosed the inaccurate data to unless it would be impossible or involve disproportionate effort. We will let you know who those third parties are on request.

Please note, we do not have to change data just because you disagree with it if that was the opinion of a professional at the time. But we are required to add a file note saying what you dispute.

Right to erasure (right to be forgotten)

There are certain circumstances in which you have a right to have your personal data erased and certain circumstances in which you do not. This right applies where:

1. It is no longer necessary for us to hold your personal data for the purposes we collected it.
2. Where our processing of your personal data was solely based on your consent, and you have withdrawn that consent;

3. Where you object to the processing and there are no overriding legitimate grounds for the processing.
4. Where you object to the processing of your data for direct marketing purposes.
5. We have processed your personal data unlawfully.
6. We must erase your personal data to comply with a legal obligation; or
7. We have collected a child's personal data in relation to the offer of information society (online) services.

Where we have disclosed the personal data to third parties, we will inform them unless it would be impossible or involve disproportionate effort. We will let you know who those third parties are on request.

Please note: This right does not apply where we need to process your personal data:

1. To comply with a legal obligation.
2. For the performance of a task in the public interest or in the exercise of official authority.
3. For public health reasons in the public interest.
4. For archiving purposes in the public interest, scientific or historical research or statistical purposes, where erasing the data would make it impossible or seriously affect our ability to achieve the aims of the processing; or

To take legal action or defend legal claims.

Right to restriction of processing

In certain circumstances you have the right to stop us from further processing your personal data. This right applies where:

1. You challenge the accuracy of the personal data. In such cases we will stop processing your personal data until we have confirmed it is accurate.
2. Our processing is unlawful, and you choose to restrict processing rather than have us erase your personal data;
3. Where we no longer need the data and intend to delete it, but you ask us to keep it for the establishment, exercise, or defence of a legal claim; or
4. Where you have objected to the processing of your data and are awaiting a decision on whether the legitimate grounds, we have claimed for the processing override yours.

Where we have disclosed the personal data to third parties, we will inform them unless it would be impossible or involve disproportionate effort. We will let you know who those third parties are on request.

Except for storing your personal data if we have agreed to restrict processing, we will only process the data with your consent or for the establishment, exercise, or defence of legal claims or for the protection of the rights of another person or for reasons of important public interest or UK law.

We will inform you inform you before the restriction of the processing is lifted.

Right to Data Portability

The right to data portability enables you get a copy of your personal data in a commonly used machine-readable format for your own use, for example, to transfer to another service provider or organisation. Where technically possible you have the right to have the data transferred directly to another service provider or organisation. This right applies in cases where you have provided the personal data, the processing is based on your consent and carried out by automated means.

Right to object

You have the right to object to the processing of your data in relation to a task we are undertaking in the public interest or in the exercise of official authority. Where you do object we will stop processing your data unless we are able to demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or we need to process the information to establish, exercise or defend a legal claim.

You have the right to object to the processing of your personal data for direct marketing, including profiling relating to direct marketing. Where you object to processing on this basis we will stop processing your personal data immediately.

You also have the right to object to the use of your personal data for scientific or historical research or statistical purposes on grounds, unless the processing is necessary for the performance of a task undertaken in the public interest.

Right not to be subjected to automated decision making

This right provides a safeguard against a potentially damaging automated decision, including profiling, being made about you without human intervention; in cases where the decision produces a legal of similarly significant effect. We will notify you of any automated decision making of this nature. We will also provide you with the contact details of a person who you can contact for an explanation of the decision. You will be able to inform that person of your point of view and ask them to revisit the decision considering what you have told them. This right does not apply if the decision is necessary for entering into or the performance of a contract, is authorised by law or you have consented to the decision being made by automated means.

How we will respond to your request to exercise your rights

Where you make a request to exercise one of your rights detailed above, we will need to confirm your identity and whether we hold your personal data. Where we do hold your personal data, we will respond to your request without undue delay and in any event within one month of your request. We may need to extend the time by a further two months depending on the complexity and number of requests. If we do need to extend the timescale, we will inform you within one month of receiving your request and let you know the reason for the delay.

This service is free of charge, however, where we consider your request to be manifestly unfounded or excessive, where it is a repeat request, we may charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested. We may also refuse to act upon your request.

Notifying you of a data protection breach

In the event we breach your data protection, and that breach is likely to result in a high risk to your rights and freedoms we will notify you of the breach without undue delay. We will explain to you clearly and in plain language the nature of the breach and provide you with the contact details of our Data Protection Officer or other point of contact from whom you can obtain further information.

We will explain the likely consequences of the breach and what we have done to address the breach and reduce the possible impact on you. We may also suggest things you may want to do to reduce the potential impact on you.

Where we have implemented technical or organisational measures, for example, used encryption software that would prevent the information being read, or taken action to ensure the potential high risk to you is unlikely to materialise, we may not inform you of the breach.

Where contacting you directly would involve disproportionate effort, for example, in cases where lots of people are affected, we may issue a public communication or similar measure to ensure you are informed in an equally effective manner. while that is the case you do have the right to make further requests for your personal data following a reasonable passage of time to exercise your right to be aware of, and verify, the lawfulness of our processing.

If we fail to act upon your request, we will inform you within one month of the reasons why we did not act and advise you of your right to make a complaint to the ICO or seek a judicial remedy.