Data Protection Policy

Adopted Date: **25/11/2019**

Review Date: **25/11/2021**

This policy needs to be read in conjunction with the Safeguarding Policy. The terms of the Safeguarding Policy are to take precedence over the guidelines set down in any other policy.

1. Introduction

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected and used fairly, stored safely and not disclosed unlawfully.

This policy complies with data protection law and follows good practice. It applies to all personal data, regardless of whether it is in paper or electronic format, and to all staff employed by our school. It also applies to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. The school was last registered on 13/03/2002 and is due to renew on 12/03/2019.

2. Definitions

Term	Definition	Example
Personal data	Information relating to a natural identifiable person, whether directly or indirectly.	- John Smith was born on 1/1/2012. - The head teacher's salary is £60,000
Data subject	The person who the data belongs to.	- John Smith the pupil - Jane Smith the teacher
Special categories of personal data	Personal data which is more sensitive and so needs more protection. We treat FSM, SEN and safe guarding data as special category data in accordance with best practice recommendations.	- Racial or ethnic origin - Political opinions - Religious or philosophical beliefs - Trade union membership - Genetics - Biometrics (e.g. fingerprints), used for identification purposes - Health – physical or mental - Sex life or sexual orientation - Data relating to criminal offences
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.	We process data relating to parents, pupils, staff, governors, visitors and others and we are a data controller.
Processing	Anything done to personal data. Processing can be automated or manual.	Collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.
Data processor	A person or organisation who processes personal data on behalf of the data controller. This can be a member of staff, 3rd party company or another organisation.	- Payroll provider - Confidential waste disposal company - Local Authority.
Personal data breach	Personal data that has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed or made available where it should not have been.	- Sending a list of pupil names, attainment marks and dates of birth to the wrong school. - Losing a laptop or USB - Sharing individual's email addresses by not using Bcc.

Subject access request (SAR)	Individuals have the right to access the data held about them. We have to provide the data requested within one calendar month of the request.	"I want to know the attendance data you hold about my son."

3. Roles and responsibilities

The Governing Body will:

- Establish and maintain a positive data protection culture.
- Appoint a Data Protection Officer and provide adequate resources and support for them to fulfil their statutory duties.
- Allocate sufficient resources for data protection, e.g. in respect of training for staff, encryption technology for devices.
- Monitor and review data protection issues.
- Ensure that the school provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities.
- Review and act upon data protection compliance reports from the Data Protection Officer.

The Headteacher will:

- Promote a positive data protection culture.
- Ensure that all staff co-operate with the policy.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to protect the data that they are processing.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.
- Monitor the work of the Data Protection Officer to ensure they are fulfilling their responsibilities.

All staff are responsible for:

a) Ensuring that:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use;
- Papers containing confidential personal data are not left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- Personal data is not in the view of others when being used;
- Locking their computer screens when unattended;
- Personal data is only held on the school network or a school issued device (laptop, USB memory stick or other removable media) which is encrypted, password protected, kept in a locked location when not in use;
- Passwords are not shared;
- Passwords comply with the complexity requirements, are changed regularly and different passwords are used for separate systems and devices;
- Personal data is only shared where necessary and in accordance with school policy, internally by sending a link to a document on the network, externally using encrypted email;
- Personal data is not disclosed accidentally or otherwise, to any unauthorised third party;

- Personal data is securely disposed of when it is no longer required and in accordance with the data retention schedule.

b) Informing the school of any changes to their personal data, such as a change of name, address, or updated relevant medical circumstances;

c) Contacting the DPO if they:

- receive a Subject Access Request
- have questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- have any concerns that this policy is not being followed
- are engaging in a new activity that involves personal data
- need help with any contracts or sharing personal data with third parties.

d) Following the data breach reporting process in the event of discovering a data breach.

4. Data Protection Officer (DPO)

As a public body, we are required to appoint a Data Protection Officer (DPO). At Hadleigh Community Primary School the DPO role is fulfilled by Tracey Riches, Clear 7 Consultancy.

The role of the DPO is to:

- Inform and advise the school/academy and the employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws.
- Be the first point of contact for supervisory authorities.
- Coordinate training on data protection for all key stakeholders.

5. Data protection principles

The GDPR states that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how we aim to comply with these principles.

5.1 Lawfulness, fairness and transparency

We will only process personal data where we have a lawful basis (legal reason) to do so. Under data protection law there are 6 lawful bases (listed in order of relevance):

a) Public task: processing is necessary so we can carry out our official functions
b) Legal obligation: the processing is necessary so we can comply with the law.
c) Contract: processing is necessary to fulfil a contract with the individual, or because they have asked the school to take specific steps before entering into a contract
d) Consent: the individual (or their parent/carer when appropriate) has freely given clear consent

e) Vital interests: the processing is necessary to protect someone's life
f) Legitimate interests: *not applicable to public authorities.*

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

5.2 Purpose and limitation

We will collect personal data for specified, explicit and legitimate reasons. We explain the data we collect, the purpose and lawful basis for collection in our privacy notices.

5.3 Accuracy and retention

We will endeavour to ensure that the data we store is accurate and up to date.

We undertake an annual exercise to check the data we hold is correct (e.g. name, address, phone number, next of kin details, emergency contact and other essential information). This exercise also provides individuals with the opportunity to review the consent they have given for the school.

Parents/carers and staff are also requested to inform the school when their personal information changes.

We securely destroy data in accordance with our Data Retention schedule (Appendix 2).

6. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- We need to liaise with other agencies; – we will seek consent where necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils, for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

7. Subject access requests and other rights of individuals

7.1 Subject access requests (SAR)

Our privacy statements provide an outline of the personal data we hold, why we hold it and who we share it with.

Individuals have a right to make a 'subject access request' to request a copy of the personal information that we hold about them.

To help individuals exercise this right we provide a form on our website. Hard copies of the form can be requested from the school office. We ask that SARs are made using the form so that we can ensure that we provide the information requested however subject access requests can also be made verbally or by letter or email.

If staff receive a subject access request they must immediately forward it to the DPO, via the Head or School Business Manager.

Appendix 1 provides more information about SARs.

7.2 Other data protection rights of the individual

Individuals also have the right to:

- Withdraw their consent to processing at any time, where consent is used as the legal basis for processing.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

8. Parental requests to see the educational record

Parents, or those with parental responsibility, may request access to their child's educational record, which will be provided at the discretion of the Headteacher within 15 school days of receipt of a written request.

9. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using a unique PIN if they wish.

Consent can be withdrawn at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

10. Photographs and videos

Each year we will ask for written consent from parents/carers to allow the photography of pupils and the specific use of these images, for example:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, unless we have permission to do so, to ensure they cannot be identified.

See our Policy for more information on our use of photographs and videos.

11. CCTV

We currently do not use closed circuit television (CCTV).

If we did, CCTV images would be used to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the school property. The school would have a CCTV policy in place which documents:

- why CCTV is used
- where cameras are sited
- whether covert monitoring is undertaken
- how long images are retained for
- who has access to the images.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third- party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

13. Personal data breaches

Despite our best endeavours a data security breach could still happen. Examples include:

- Human error (e.g. sending an email to the wrong person/s, sharing individual's email addresses by not using Bcc, posting information to the wrong address, dropping/leaving paperwork containing personal data in a public space)
- Loss or theft of equipment containing personal data (e.g. Laptop, USB stick, mobile phone). Note this is a breach even if the device is encrypted.
- Equipment failure
- Fire, flood
- Hacking attack
- "Blagging" offences where personal data is obtained by deceit.

In the event of a breach, we will follow our Personal Data Breach Procedure.

14. Training

All staff and other key stakeholders (e.g. governors, volunteers) will be made aware of their responsibilities for data protection as part of their induction programme.

Refresher training will take place annually in the Autumn Term.

A central training record will be maintained.

15. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- E-safety Policy
- Policy for Child Protection and Safeguarding Children
- CCTV (N/A at present)

Appendix 1: Subject Access Requests

Individuals have a right to make a 'subject access request' to request a copy of the personal information that we hold about them.

We provide a form to help individuals exercise this right. This can be found in on the next page and on our website. Hard copies of the form can be requested from the school reception. Subject access requests can also be made verbally or by letter or email.

If staff receive a subject access request they must immediately forward it to the DPO.

Personal data about a child belongs to that child, and not the child's parents or carers.

For a parent or carer to make a subject access request in respect of their child we consider whether the child is mature enough to understand their rights.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. The Gillick competency guidelines would be applied to this understanding. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

On receipt of a SAR we may ask for 2 forms of identification, for example a passport and utility bill.

We will also:

- confirm the request in writing and our understanding of the information requested
- respond without delay and within 1 month of receipt. Where a request is complex or numerous we may extend this to 3 months. We will confirm this within 1 month, and explain why the extension is necessary

In certain circumstances we may not disclose information. When we refuse a request, we will explain why, and provide information on how to complain to the Information Commissioners Office.

There is generally no charge for a SAR. However, if the request is considered to be 'manifestly unfounded or excessive' we may charge an administration fee or refuse to provide the information. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

We maintain a register of SAR received to enable us to monitor this.

Subject Access Request Form

This form is intended to support individuals with their requests for personal data and to help us ensure that we provide the information that is being requested.

1. Whose data is being requested?	
Name	
Address	
Relationship with the school For example: Pupil, employee, governor, parent, volunteer	
2. Who is making the request?	
Name	
Address (if different from above)	
Telephone	
Email	
Are you requesting your own data? If yes, go to Section 3	Yes/No
If no, what is your relationship with the person whose data is being requested?	
3. What information is being requested?	
Are you looking for anything specific? For example: • Your personnel file • Your child's medical records • Your child's behaviour record • Emails between 'A' and 'B' between [date]	
Is there a particular time period you are interested in?	
Is there anyone specific we should talk to?	
How would you like the information to be provided? For example: email, verbally, by post	
Signed:	
Date:	

Please forward to:

DPO for Hadleigh Community Primary School via the school's Data Protection Lead or School office.

If sending electronically, please use email address:

gdpr@hadcps.uk

Appendix 2: Document retention schedule

Extract from the Information Management Toolkit for school 2016

Record	Personal Data Category	Retention Period
Governance and Management		
Governor details	Personal data	For the duration of their term of office (max 4 years)
Register of interests (governors and staff)	Personal data	6 years + current
Minutes of Governors Meetings (including confidential minutes/reports)	Special categories of personal data	PERMANENT
Delegation arrangements and committees	N/A	
Minute/notes of meetings of SMT	N/A	Date of the meeting + 3 years
Reports created by SMT	N/A	Date of the report + 3 years
Records created by SMT	N/A	Current year + 6 years
Correspondence created by SMT	N/A	Date of the correspondence + 3 years
Policy documents and action plans	N/A	Life of the report/policy + 3 years
School Development Plan	N/A	Life of the report/policy + 3 years
Proposals relating to the change of status of a maintained school	N/A	Date proposal accepted or declined + 3 years
Records of complaints dealt with by the Governing Body	Special categories of personal data	Date of the resolution of the complaint plus a minimum of 6 years
Annual Parents Meeting papers	N/A	Date of the meeting + 6 years
Records relating to creation of school brochure/website	N/A	Current year +3
Records relating to circulars to staff, parents or pupils	N/A	Current year + 1
Newsletters	N/A	Current year + 1
Visitors' signing in book/management system	Personal data	Current year + 6 years
Biometric system - registration	Special categories of personal data	Current year + 6 years
Pupils		
Admissions paperwork	Special categories of personal data	Date of admission + 1 year
Unsuccessful admissions	Special categories of personal data	Until appeals process is completed
Pupil personal details (Management Information System)	Special categories of personal data	
Pupil's Educational Record (Curriculum blue file)	Personal data	Primary schools: retain until point of transfer Secondary: DOB + 25 years

Special educational needs data (EHCP)	Special categories of personal data	DOB + 25 years
Child Protection files	Special categories of personal data	X years
General consent form	Special categories of personal data	
Parent/carer contact details	Personal data	Deleted as soon as child leaves the school
Consent forms - residential off-site activities	Special categories of personal data	
Educational visit paperwork (risk assessments, EHCP, parental contact details, SEN data)	Special categories of personal data	
Images of pupils on MIS system and shared for medical purposes	Personal data	
Walking bus registers	Personal data	Date of register + 3 years
Behaviour incidents	Personal data	
Accident reports	Personal data	
Attendance registers	Personal data	3 years after the date on which the entry was made
Authorised absence records (Holiday forms)	Personal data	Current academic year + 2 years
SATS results	Personal data	X years from when the pupil leaves school
Assessment results and records of pupil progress	Personal data	
Reports to parents	Personal data	
Curriculum Management		
Curriculum returns	N/A	Current year + 1
SATS results (composite record)	N/A	Current year + 1
Schemes of work	N/A	Current year + 1
Timetables	N/A	Current year + 1
Class record books	N/A	Current year + 1
Mark books	N/A	Current year + 1
Record of homework set	N/A	Current year + 1
Pupils work	N/A	Current year + 1
Staff		
Single central record	Personal data	

All records leading up to the appointment of a new member of staff	Special categories of personal data	Termination of appointment + 6 years
Pre-employment vetting information - DBS Checks	Personal data	MAXIMUM 6 months
Pre- employment vetting information - evidence proving the right to work in the UK	Personal data	Termination of appointment + 2 years MINIMUM
Staff Personal File	Special categories of personal data	Termination of appointment + 6 years
Performance/CPD data	Personal data	Current year + 5 years
Staff e-learning contract	Personal data	
Timesheets, sick pay	Special categories of personal data	Current year + 6 years
Occupational Health referrals	Special categories of personal data	
Maternity pay records	Personal data	Current year + 3 years
Disciplinary records	Personal data	
Health and Safety		
Minor incident log relating to children	Special categories of personal data	
Incident Report Form - children	Special categories of personal data	DOB + 25 years
Incident Report Form - adults	Special categories of personal data	Date of incident + 12 years (longer for serious accidents
HSE Accident reporting - Adults	Special categories of personal data	Date of incident + 6 years
CCTV recordings	N/A	N/A
Health and safety policy statements	N/A	Life of policy + 3 years
Health and safety risk assessments	N/A	Life of risk assessment + 3 years
Control of Substances Hazardous to Health (COSHH)	N/A	Current year + 40 years
Asbestos log book	N/A	Last action + 40 years
Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	N/A	Last action + 50 years
Fire precaution log books (including fire risk assessment)	N/A	Current year + 6 years
Financial Management of the School		
Employer's Liability Insurance Certificate	N/A	Closure of the school + 40 years
Inventories of furniture and equipment	N/A	Current year + 6 years
Burglary, theft and vandalism report forms	N/A	Current year + 6 years
Annual accounts	N/A	Current year + 6 years
Loans and grants managed by the school	N/A	Last payment + 12 years

Budget plan and associated paperwork	N/A	Current year + 6 years
Cashless payment systems	Personal data	Deleted as soon as child leaves the school
Invoices, receipts,	N/A	Current year + 6 years
Requisitions and delivery notes	N/A	Current year + 6 years
Debt incurred, e.g. Dinner Money	Personal data	Current year + 6 years
Staff cost calculations for budget setting	Personal data	Current year + 6 years
Staff members' bank details	Personal data	Current year + 6 years
School letting information	Personal data	Current year + 6 years
School fund records	N/A	Current year + 6 years
Contract records	N/A	Last payment + 6 years (unless under seal)
Contract monitoring records	N/A	Current year + 2 years
Student Grant applications	Personal data	Current year + 3 years
Free School Meals Registers	Personal data	Current year + 6 years
School Meals Registers	Personal data	Current year + 3 years
Property Management		
Title deeds of property	N/A	PERMANENT
Plans of property	N/A	PERMANENT
Leases of property leased by the school	N/A	Expiry of lease + 6 years
Records relating to letting of the school premises (lettings policy, booking form, insurance, safeguarding policy)	N/A	Current year + 6 years
Records relating to the maintenance of the school by contractors and employees (Premises Log Book)	N/A	Current year + 6 years

End of Data Protection Policy