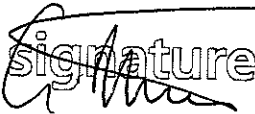



Howard Park Community School
General Data Protection Regulations Policy

GDPR

November 2018

 signature	 signature
Date: 8-2-19	Date: 8/2/19
Chair of Governors	Head Teacher

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Definitions	3
4. The data controller	4
5. Roles and responsibilities	4
6. Data protection principles.....	5
7. Collecting personal data.....	5
8. Sharing personal data.....	6
9. Subject access requests and other rights of individuals	6
10. Parental requests to see the educational record	8
11. CCTV.....	8
12. Photographs and videos	8
13. Data protection by design and default	8
14. Data security and storage of records.....	9
15. Disposal of records	9
16. Personal data breaches	10
17. Training.....	10
18. Monitoring arrangements	10
19. Links with other policies	10
Appendix 1- Subject Access Request Form.....	11
Appendix 2- Permission for walks, internal and external photos	14
Appendix 3 - GDPR Rules within school	15
Appendix 4 - Personal Data Breaches	18

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
<p>Personal data</p>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<p>Special categories of personal data</p>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy

- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say 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 the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

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.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's [retention policy and schedule – see append].

8. 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 as 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.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should be made by completing a SAR request form (See Appendix 1) or by emailing the school office which should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO. During the summer break staff will not be available to deal with SARs until the new term commences.

9.2 Children and subject access requests

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 with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- 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.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Anyone who believes that they have been filmed by CCTV, is entitled to ask for a copy of the data, subject to exemptions contained in the Act. **They do not have the right of instant access.**

The Data Protection Processor will then view the data and decide if access to the data and/or a copy is to be provided to the applicant. If access to the specified data or a copy is to be provided, a decision should also be made regarding the need to seek consent or conceal the identity of other parties shown in the images deemed necessary.

The Act gives the school the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for internal and external photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph and not distribute it further. The only exception being pre-published marketing materials, which we have already been printed. These will not be reprinted without first removing the photograph.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified. See appendix 2.

13. 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 (see section 6)
- 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

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- 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 must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

See the Data Retention and Schedule for further details. All school staff are provided with GDPR Rules within School (see appendix 3).

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 4.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every **2 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Acceptable Use Policy
- Safeguarding
- Retention guide & schedule

Appendix 1

Please visit www.howardpark.co.uk/sar/ for access to this form

Appendix 2

The letter requesting permission for such activity is included in our admissions form and is asked annually thereafter during our data update period.

Appendix 3

GDPR Rules within school

Reports

- Working on:
 - When working on reports this should only be completed on school computers within school, encrypted laptops at home or personal laptops IF the report is saved on an encrypted stick.
 - When working on reports on a computer/laptop, if leaving the device, the screen must be locked with a password protected entry.
- Saved:
 - Reports should only be saved on encrypted memory sticks or school server.
 - Front pages of reports (containing images of children) should only be saved on the school server and not accessed elsewhere.
- Sharing:
 - When sharing reports with SLT- these should NOT be emailed but saved on the school server for checking or transferred via an encrypted memory stick.
- Paper copies
 - Paper copies of reports should not leave school premises and be kept in a cupboard within the classroom. Paper copies of reports in classrooms should be destroyed within 1 year.
 - A paper copy of reports should also be kept in the school office in a locked cupboard.
 - Paper copies of reports should not be left on desks or around school at any time.
 - Drop files- more information will follow, as we are likely to shred these.

Pupil images

- Pictures should be deleted 2 years after using them
- Taking pictures:
 - Pictures of children should only be taken on school devices such as cameras, iPads etc.
 - Only pictures of children with consent should be taken.
 - If taking devices outside of school to take photos e.g trips; only images of external photo permission children should be taken. Images of internal photo children should be deleted from the device prior to taking the device out of school.
 - Pictures on devices deleted within 2 months- ideally as soon as downloaded.
- Saved:
 - Pictures should only be saved on the school server and not on any external storage device.
 - Pictures of children with external consent may be saved on encrypted memory sticks.
 - If pictures, of children with only internal consent, need to be saved on encrypted memory sticks the permission of the head must be sought after.
- Sharing:
 - Pictures of children should only be stored on the school server or encrypted memory stick (if external consent obtained).
 - The pictures of children who have provided external photograph permission can be shared via the school email (not personal email).
 - Pictures of children who have external photograph permission can be included on perspective as part of performance management meetings.
- Paper copies

- Paper copies of pictures of children with only internal consent should not leave school premises.
- Paper copies of pictures in classrooms should be destroyed within 1 year. (2 years for nursery)

Intervention details (PP/PM)

- Working on:
 - When working on intervention documents (Pupil Premium Plans/ Provision Maps/ SEN records) this should only be completed on school computers within school, encrypted laptops at home or personal laptops IF the document is saved on an encrypted stick.
 - When working on intervention documents on a computer/laptop, if leaving the device, the screen must be locked with a password protected entry.
- Saved:
 - Intervention documents should only be saved on encrypted memory sticks or school server.
- Sharing:
 - When sharing Intervention details with SLT- these should NOT be emailed but saved on the school server for checking or transferred via an encrypted memory stick.
- Paper copies
 - Paper copies of records should not leave school premises and be kept in a cupboard within the classroom. Paper copies of reports in classrooms should be destroyed within 1 year.
 - If intervention details are required longer than 1 year they are to be kept in the school office in a locked cupboard.
 - Paper copies of reports should not be left on desks or around school at any time.

Assessment data

- Working on:
 - When working on assessment documents this should only be completed on school computers within school, encrypted laptops at home or personal laptops IF the document is saved on an encrypted stick.
 - When working on assessment documents on a computer/laptop, if leaving the device, the screen must be locked with a password protected entry.
- Saved:
 - Assessment should only be saved on encrypted memory sticks or school server.
- Sharing:
 - When sharing assessment details with SLT- these should NOT be emailed but saved on the school server for checking or transferred via an encrypted memory stick.
- Paper copies
 - Paper copies of records should not leave school premises and be kept in a cupboard within the classroom. Paper copies of assessment in classrooms should be destroyed within 1 year.
 - SLT to keep paper copies in files
 - If intervention details are required longer than 1 year they are to be kept in the school office in a locked cupboard.
 - Paper copies of reports should not be left on desks or around school at any time.

E-mails

- If staff access emails using personal devices, controls must be in place (more information will follow as this requires more than your phone password)
- Received emails deleted after 2 years of receiving them

- Sent emails deleted after 2 years of receiving them
 - If the information is still needed it should be copied and placed in your documents

Please note as part of GDPR if you are away from your screen then you MUST lock the screen

Do not share passwords

If allowing someone to use your login details then you must be present as you are held answerable for your account

Issued to all teaching and support staff 2 May 2018

Appendix 4 1.0 Introduction

Personal Data Breach – Reporting Procedure

From May 2018 the EU's General Data Protection Regulation and the Data Protection Act 2018 came into force. As part of this legislation, a new process has been written to inform Warwick Road Primary School employees what to do if they discover an information security incident (personal data breach).

2.0 Scope

This policy applies to all Howard Park Community School employees, any authorised agents working on behalf of Howard Park Community School, including temporary or agency staff, elected members, and third-party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action. This applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

3.0 Notification and Containment Article 33 of the GDPR compels data controllers to report breaches of personal data, to the Information Commissioner's Officer, within 72 hours of discovery, if the incident is likely to result in a risk to the rights and freedoms of data subjects. Therefore it is vital that Warwick Road Primary School has a robust system in place to manage, contain, and report such incidents.

3.1 Immediate Actions (Within 24 Hours) If an employee, governor, or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to the Business Manager within 24 hours. If the Business Manager is not at work at the time of the notification then the Headteacher will start the investigation process. If appropriate, the officer who located the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

3.2 Assigning Investigation (Within 48 Hours) Once received, the Business Manager will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are:

WHITE Information security event
No breach has taken place but there is a failure of the implemented safeguards that could cause a data breach in the future.
GREEN Minimal Impact
A data breach has occurred but has been contained within the organisation (or trusted partner organisation), the information is not considered to be particularly sensitive, and no further action is deemed necessary.
AMBER Moderate Impact
Security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the information commissioner's office.
RED Serious Impact
A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the information commissioner's office and urgent remedial action. HR input may also be required.

The Business Manager will notify the ICT Co-Ordinator (ICTC) that the breach has taken place. The Business Manager will recommend immediate actions that need to take place to contain the incident. The ICTC will investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistance of Internal Audit and Counter Fraud Teams.

3.3 Reporting to the ICO/Data Subjects (Within 72 Hours)

The ICTC, in conjunction with the Business Manager and DPO will make a decision as to whether the incident needs to be reporting to the ICO, and also whether any data subjects need to be informed. The Business Manager will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

4.0 Investigating and Concluding Incidents

The Business Manager will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented. When the DPO has investigated a data breach then the ICTC must sign off the investigation report and ensure recommendations are implemented across the Council.

The ICTC will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed. The Headteacher will be kept informed at all stages.

Queries about any aspect of the school's Information Governance strategy or corresponding policies should be directed to the Data Protection Officer at hello@howardpark.co.uk.