

Data Protection Policy

Navigation Primary School

Navigation Primary



Working together, learning together

Approved by:

FINANCE, PERSONNEL &
FACILITIES COMMITTEE

Date: 19/06/19

Last reviewed on:

March 2019

Next review due by:

SUMMER 2021

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	6
8. Sharing personal data.....	6
9. Subject access requests and other rights of individuals	7
10. Parental requests to see the educational record	8
11. Photographs and videos	8
12. Data protection by design and default.....	9
13. Data security and storage of records	9
14 Disposal of records.....	10
15. Personal data breaches	10
16. Training	10
17. Monitoring arrangements.....	10
18. Links with other policies	10
Appendix 1: Personal data breach procedure	11
.....	

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
Personal data	<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>
Special categories of personal data	<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• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes• Health – physical or mental• Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>

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.
Data protection Impact Assessment (DPIA)	DPIAs are tools to identify the risks in data processing activities with a view to reducing them.

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, external organisations or individuals working on our behalf. Staff members who do not comply with this policy may face disciplinary action. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

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 the school's compliance with data protection law and developing related policies and guidelines where applicable.

The DPO 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.

Our DPO is **Judicium Education** - contactable via

dataservices@judicium.com

72 Cannon Street London

EC4N 6AE

Lead contact Craig Stilwell

Telephone 0203 326 9174

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

- (a) If you are unsure of the lawful basis being relied on by the School to process personal data;
- (b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);
- (c) If you need to draft privacy notices or fair processing notices;
- (d) If you are unsure about the retention periods for the personal data being processed but would refer you to the NPS's data retention policy in the first instance;
- (e) If you are unsure about what security measures need to be put in place to protect personal data;
- (f) If there has been a personal data breach and would refer you to the procedure set out in NPS's breach notification policy;
- (g) If you are unsure on what basis to transfer personal data outside the EEA;
- (h) If you need any assistance dealing with any rights invoked by a data subject;
- (i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
- (j) If you plan to undertake any activities involving automated processing or automated decision making;
- (k) If you need help complying with applicable law when carrying out direct marketing activities;
- (l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

5.3 Headteacher

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

5.4 All staff

Staff members 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 Navigation Primary 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 six '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, NPS will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If NPS offers 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).

Whenever NPS first collects personal data directly from individuals, they will be provided with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

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

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

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

When staff members 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, which is linked to the guidance set out in the IRMS toolkit.

8. Sharing personal data

NPS 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 the staff at risk.
- NPS needs to liaise with other agencies – consent will be sought as necessary before doing this.
- NPS's suppliers or contractors need data to enable them to provide services to NPS's staff and pupils – for example, IT companies. When doing this, NPS 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.

NPS will also share personal data with law enforcement and government bodies where 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.

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

Where NPS transfers personal data to a country or territory outside the European Economic Area, it 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' 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 must be submitted in writing, either by letter, email or fax to the DPO. An individual can make a request via the NPS office and this will be passed onto the DPO. SAR should include the:

- 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.

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 NPS 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, NPS:

- may ask the individual to provide two forms of identification;
- may contact the individual via phone to confirm the request was made;
- will respond without delay and within one month of receipt of the request;
- will provide the information free of charge;
- may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous – in such a case NPS will inform the individual of this within one month, and explain why the extension is necessary.

NPS 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, NPS 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 NPS refuses a request, the individual will be told why, and that 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 NPS is collecting their data, about how it will be used and processed (see section 7), individuals also have the right to:

- withdraw their consent to processing at any time;
- ask NPS 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 members 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 fifteen school days of receipt of a written request.

11. Photographs and videos

As part of NPS's activities, photographs and video images of individuals may be taken within the school.

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

Where NPS needs parental consent, it will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where parental consent is not needed, NPS will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- 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 Twitter feed;
- on display boards within the school.

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

12. Data protection by design and default

NPS will put measures in place to show that it has integrated data protection into all of NPS's 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, and 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;
- regularly conducting reviews and audits to test NPS's privacy measures and make sure NPS is compliant;
- maintaining records of NPS's processing activities, including:
 - for the benefit of data subjects, making available the name and contact details of the school and DPO and all information NPS is required to share about how it uses and process their personal data (via privacy notices);
 - for all personal data that NPS holds, maintaining an internal record of the type of data, data subject, how and why the data is being used, any third-party recipients, how and why NPS is storing the data, retention periods and how the data is being kept secure.

13. Data security and storage of records

NPS 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 eight characters long, containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff members 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.
- Governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT policy/acceptable use agreement).
- Where it is necessary to share personal data with a third party, NPS carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. 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 NPS cannot or does not need to rectify or update it. For example, paper-based records will be shredded and electronic files will be overwritten or deleted. NPS may also use a third party to safely dispose of records on the school's behalf, in which case, NPS will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

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

In the unlikely event of a suspected data breach, NPS will follow the procedure set out in the Data Breach Policy.

When appropriate, NPS 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.
- If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches (who is the head teacher or your DPO).

16. Training

All staff members 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.

17. 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** by the FPF committee and shared with the full governing board.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Retention policy
- ICT/Acceptable use policy
- Data Breach Policy