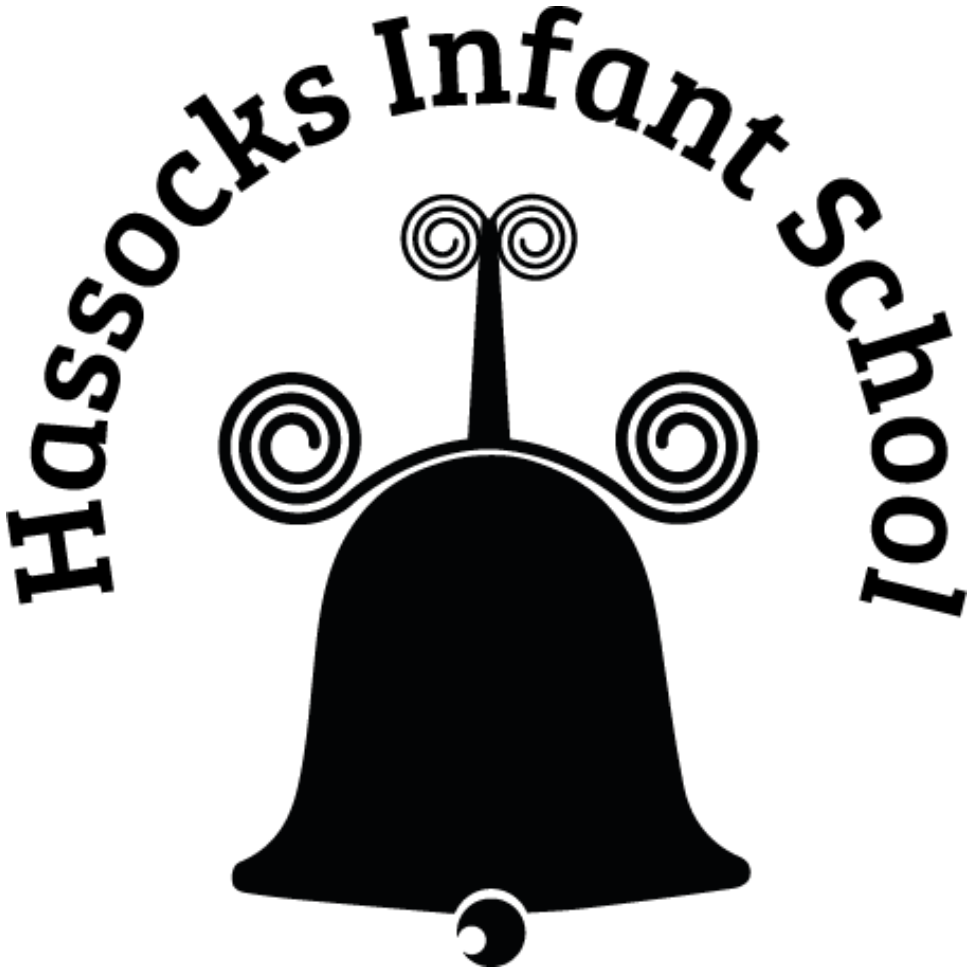
Hassocks Infant School

Data Protection Policy



✯ Explore ✯ Respect ✯ Flourish

Date policy agreed:	September 2023
Date policy to be reviewed:	Four yearly September 2027
Responsibility:	School Office with approval from Head

Hassocks Infant School
Data Protection Policy

Introduction

On the 25th May 2018 the General Data Protection Regulation (GDPR) will be applicable and the current Data Protection Act (DPA) will be updated by a new Act giving effect to its provisions. Before that time the DPA will continue to apply.

This Policy sets out the manner in which personal data of staff, students and other individuals is processed fairly and lawfully.

The School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the School. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

The School is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The School must be able to demonstrate compliance. Failure to comply with the Principles exposes the School and staff to civil and criminal claims and possible financial penalties.

Details of the School's purpose for holding and processing data can be viewed on the data protection register: https://ico.org.uk/esdwebpages/search

The Schools registration number is Z1171358. This registration is renewed annually and updated as and when necessary.

Aim

This Policy will ensure:

- The School processes person data fairly and lawfully and in compliance with the Data Protection Principles.
- All staff and volunteers involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.
- That the data protection rights of those involved with the School community are safeguarded.
- Confidence in the School's ability to process data fairly and securely.

Scope

This Policy applies to:

- Personal data of all School employees, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the School.
- The processing of personal data, both in manual form and on computer.
- All staff and governors.

The Data Protection Principles

The School will ensure that personal data will be:

1. Processed fairly, lawfully and in a transparent manner.

2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The School will be able to demonstrate compliance with these principles.

The School will have in place a process for dealing with the exercise of the following rights by Governors, staff, students, parents and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record;
- to erasure;
- to restrict processing;
- to object to processing;

Roles and Responsibilities

The Governing Body of the School and the Head Teacher are responsible for implementing good data protection practices and procedures within the School and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy

A designated person, the Data Protection Officer (DPO), will have responsibility for all issues relating to the processing of personal data and will report directly to the Head Teacher.

The Data Protection Officer will comply with responsibilities under the GDPR and will deal with subject access requests, requests for rectification and erasure, data security breaches. Complaints about data processing will be dealt with in accordance with the Schools Complaints Policy. The named DPO is published on the school website and the ICO website.

Data Security and Data Security Breach Management

- All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

- Access to personal data should only be given to those who need access for the purpose of their duties.

- All staff will comply with the Schools Acceptable IT use Policy.

- Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the Acceptable IT use Policy.

- Data will be destroyed securely in accordance with the 'Information and Records Management Society Retention Guidelines for Schools'.

- New types of processing personal data including surveillance technology which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented until a Privacy Impact Risk Assessment (PIA) has been carried out. Please see Appendix A for HIS Privacy Impact Assessment Procedures and Guidance.

- The School will have in place a data breach security management process and serious breaches, where there is a high risk to the rights of the individual, will be reported to the Information Commissioner's Office (ICO) within 72 hours (in compliance with the GDPR).

- All staff will be aware of and follow the data breach security management process.

- All staff will be aware of and comply with the list of Do's and Don'ts in relation to data security in Appendix B.

Subject Access Requests

Requests for access to personal data (Subject Access Requests - SARs) will be managed by the Data Protection Officer. Generally, no fee is applicable but please refer to the Subject Access Request process for further information on fees. Records of all requests will be maintained.

The School will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time period is one calendar month of receipt of the request.

Sharing data with third parties and data processing undertaken on behalf of the School.

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the School e.g. by providing cloud based systems or shredding services, the School will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles.

Ensuring compliance

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be available to all staff.

All staff will read and sign the Acceptable Use Policy.

The School advises students whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on the School website.

The School also provides a Privacy Notice to staff which is available on the School website.

The School will ensure Privacy Notices contain the following information:

- Contact Data Controller and Data Protection Officer details
- Purpose of processing and legal basis. Retentions period. Who we share data with.
- Right to request rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable.

Photographs, Additional Personal Data and Consents

Where the School seeks consents for processing person data such as photographs at events it will ensure that appropriate written consents are obtained. Those consent forms will provide details of how the consent can be withdrawn.

Where the personal data involves a child under 16 years written consent will be required from the adult with parental responsibility.

Appendix A

Privacy Impact Assessment Procedure for Hassocks Infant School

1. Introduction

A privacy impact assessment (PIA) is a tool which can help Hassocks Infant School identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective PIA will allow Hassocks Infant School to identify and fix problems at an early project stage, reducing the associated costs and damage to reputation which might otherwise occur.

This procedure explains the principles which form the basis for a PIA.

The main body of the procedure sets out the basic steps which the School should carry out during the assessment process.

Templates are at Annex A and B

2. What is a Privacy Impact Assessment (PIA)?

A PIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a PIA should be used throughout the development and implementation of the School's project.

A PIA will enable the School to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

3. When will a PIA be appropriate?

PIAs should be applied to all new projects, because this allows greater scope for influencing how the project will be implemented. A PIA can also be useful when planning changes to an existing system.

A PIA can also be used to review an existing system, but the School needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system. The main purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met.

Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

Conducting a PIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising. A PIA should be undertaken before a project is underway.

4. What is meant by Privacy?

Privacy, in its broadest sense, is about the right of an individual to be left alone.

It can take two main forms, and these can be subject to different types of intrusion:

- **Physical privacy** - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal

possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

- **Informational privacy** – the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages
.

5. Informational Privacy

This procedure is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information.

Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to someone where the person who it is about does not want them to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information.

Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a PIA should be a minimisation of privacy risk.

6. The Benefits of a PIA

The Information Commissioner's Office (ICO) promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits.

Whilst a PIA is not a legal requirement (except 'high risk processing i.e. safeguarding data), the ICO may often ask an organisation whether they have carried out a PIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with the DPA.

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within the School and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a PIA would be appropriate

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more schools seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of the school.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications.
- The collection of new data on an existing system.

7. PIA Procedure

The format for an initial PIA is at **Annex A.**

This review form is based on the eight Data Protection Principles described in Schedule 1 of the Data Protection Act.

In the event that a full PIA is deemed appropriate the format for this is at **Annex B**

The links between the PIA and DPA are set out in **Annex C**

8. Monitoring

The completed PIA should be submitted to the Governing Body for review and approval. The Governing Body will monitor implementation of actions identified in PIA's

(Extracted from the ICO – PIA Code of Practice)

Annex A

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering ‘yes’ to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
- Will the project require you to contact individuals in ways that they may find intrusive?

(Extracted from the ICO – PIA Code of Practice)

Annex B

Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex C can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

(Extracted from the ICO – PIA Code of Practice)

Annex C

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Appendix B

What staff should do:

DO get the permission of your manager to take any confidential information home.
DO transport information electronically from school by the use of Office 365. Wherever possible avoid taking paper documents out of the office.
DO use secure portable computing devices such as encrypted laptops when working remotely or from home.
DO ensure that all paper based information that is taken off the school premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.
DO ensure that paper based information and laptops are kept safe and close to hand when taken off the school premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
DO return the paper based information to the School as soon as possible and file or dispose of it securely.
DO report any loss of paper based information to your line manager **IMMEDIATELY**.
DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.
DO ensure that when posting/emailing information that only the specific content required by the recipient is sent.
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to SIMS (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic user names such as 'Sysman' are disabled.

What staff must not do:

DO NOT use USB memory sticks to transfer data between school and home or internally to transfer data between machines in school. Office 365 should be used for all document management in school and at home.
DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
DO NOT unnecessarily copy other parties into e-mail correspondence.
DO NOT e-mail documents to your own personal computer.
DO NOT store work related documents on your home computer.
DO NOT leave personal information unclaimed on any printer or fax machine, this includes class lists, assessment information, ILP's, EHCP's and reports.
DO NOT leave personal information on your desk overnight, or if you are away from your desk in meetings.
DO NOT leave documentation in vehicles overnight.
DO NOT discuss case level issues at social events or in public places.
DO NOT put confidential documents in non-confidential recycling bins.
DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.