Data Protection Policy

The school collects and uses personal information, referred to in the Data Protection Act, 2018 (referred to hereafter as "UK GDPR") as personal data, about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and for administrative functions. In addition, the school is also required by law to collect, use and share certain information.

The school is the recognised Data Controller, of the personal information that it collects and receives for these purposes. The term Data Controller is used to describe an organisation that collects and determines the purposes and means of processing personal data.

The school issues Privacy Notices for pupils (including parents and carers) and staff. These summarise the personal information held by the school, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data.

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the UK GDPR, and other related legislation. This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/data?

The UK GDPR refers to 'personal data' as meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

The UK GDPR refers to sensitive personal data as "special categories of personal data". The table below lists a range of data types, identifying the differences between personal and special category data, but is not limited to this list.

Personal Data	Special Category Data
• Persons name	• Genetic
• Address/location	• Biometric
• Identification number	• Racial or ethnicity
• Online identifier	• Political opinions
• Physical identity	• Religious or philosophical beliefs
• Physiological or behavioural	• Trade union membership
• Economic	• Health or sex life
• Cultural or social	• Sexual orientation

Article 9, paragraph 1 of the UK GDPR prohibits the processing of any type of "Special Category Data" except in specified circumstances. For the school's purposes, we are permitted and legally obliged to process special category data for the purposes of "specific public interest" (Article 9, paragraph 2g), such as the Department for Education's (DfE) annual School Census.

Data Protection Principles

The UK GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner;

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes);

3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive;

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

5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Personal data shall be processed (i.e. used, stored, deleted) in a manner that ensures appropriate security of the data at all times.

Duties

Personal data shall not be transferred to a third country or territory outside the UK, unless that country or territory ensures an adequate level of data protection. Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties of the UK GDPR at all times. Therefore the school will:

1. **Inform individuals of the identity and contact details of the designated lead for data protection**. This information can be found at the end of this Data Protection Policy and on the school Privacy Notices. The school office can also provide this information on request.

2. **Inform individuals of the purposes that personal information is being collected and the basis for this.** This information can be found in depth within this Data Protection Policy, in the school Privacy Notices and in a more concise version on school consent forms.

   The collection and use of the personal data of pupils, parents and staff is conducted to allow the school to perform its contractual obligations, official functions, public interest tasks and other legal responsibilities. The statutory provisions covering these areas include the following:

   - The Education Act 1996
   - The Education (Pupil Information) (England) Regulations 2005
   - Schools Admission Code 2014
   - 'Keeping Children Safe in Education' 2016: Department for Education

The school takes part in official data collection activities, such as school censuses, phonics screening checks, EYFS and key stage 1 assessments amongst others. In these instances the school has a legal obligation to supply this data, however we also share data with third party processors to allow us to fulfil our day to day management of school processes and to provide educational resources. All of our third party processors have to demonstrate that they are compliant with the UK GDPR and that they have adequate procedures in place to protect the school's data.

We use pupil data to:

- support pupil learning
- monitor and report on pupil progress
- provide appropriate pastoral care
- assess the quality of our services
- comply with the law regarding data sharing

If the school does not have a legal basis to collect or use certain types of data (the use of pupil photos in the school newsletter, etc), the school will always seek explicit consent to control and process the data in compliance with the UK GDPR.

3. **Inform individuals when their information is shared, and why and with whom unless the UK GDPR provides a reason not to do this.** This policy identifies the reasons why personal data is shared and in what context. The school are currently updating all of the consent forms to show why the information is being collected, how it will be used and if any third party processors are involved. Third Party processors are used to help the school manage its information for administration purposes, such as Centrally Hosted SIMS, School Cash Office, etc or to support pupil learning with platforms such as Purple Mash, Speech Link or Tapestry. The school will only share the minimum level of data required to achieve the desired purpose or outcome.

4. **If the school plans to transfer personal data outside the UK the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.** The school is reviewing existing data stored off site to ensure it meets with changes to the UK GDPR regarding transfer of data outside the UK, where prior to Britain's exit from the EU the clause was "outside of the EEA". If there are any changes, the school will conduct a Privacy Impact Assessment to ensure we are confident that sufficient data protection safeguards are in place and make any adaptions or notifications as necessary.

5. **Inform individuals of their data subject rights.** The school provides privacy notices on the school website and in hard copy available from the school office. The privacy notices outline the general rights of data subjects and give directions on where to seek further information, both from the school and from external sources.

6. **Inform individuals that they may withdraw consent for data processing, where that data is not required by law.** If consent is withdrawn the school will cease processing their data although that will not affect the legality of data processed up until that point. Initial information on this process is listed in the privacy notices and more detailed guidance will be available from the school office. It is important to recognise that the school will continue to process data where required by law.

7. **Provide details of the length of time an individual's data will be kept.** The school follow Hampshire's School Records Retention Schedule, which is kept in the school office. An overview of the retention dates for most data asset types are listed on each privacy notice. The school will also provide this information on consent forms where relevant.

8. **Inform and seek consent should the school need to use data for a different purpose than it was originally collected for.** The school will always contact parents to let them know ahead of any change of use of data and will also seek explicit consent for that change of use. The school may contact parents via a range of communication tools, such as Parentmail, email or telephone, but we will always require written, signed consent.

9. **Check the accuracy of the information the school holds and review it at regular intervals.** The school monitors and updates its information as part of ongoing practice, as well as renewing its data collection sheets annually – January for Year R and September for Key Stage 1. New Year R parents submit registration forms between June and September which are used until the Data Collection Sheets are sent out in January.

10. **Ensure that only authorised personnel have access to the personal information in whatever medium (paper or electronic) it is stored in**. The school has rigorous policies to control access at various security levels. In the case of the schools IT systems, there is multitiered access from visitor, college student and Library Helper logins with no access to server data, through support staff, Teaching staff and office staff access levels, up to senior management accounts. Access to paper data is also closely controlled using lockable storage and offices.

11. **Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect against loss, theft and unauthorised disclosure, irrespective of its format.** In addition to the above commitment, we have stringent controls in place to keep our data as secure as possible. The school has a range of policies which detail how our IT infrastructure is structured to prevent unauthorised access, which contains an Acceptable Use Policy that all staff sign and agree to. We also have a "Staff IT and Data Protection Procedure Manual" which further reinforces these policies.

    All staff receive regular training and updates on IT and data security, which is constantly reviewed to produce resources and strategies to keep data protection at the forefront of all data processing activities by staff.

12. **Ensure that personal information is not retained longer than it is needed.** As stated above, the school follow the Hampshire's School Records Retention Schedule and securely dispose of documents that fall outside of their retention period. The Network Manager monitors the age of data stored on the school's IT systems and reports back to staff on their responsibilities and actions to be taken where required. Likewise, the Business Manager monitors the age of data stored in the school's archives and information management systems. Occasionally there may be a legal requirement for the school to retain data longer than the retention schedule states, such as the temporary ban on destroying material relevant to the Independent Inquiry into Child Sexual Abuse (IICSA, 2015).

13. **Ensure that when information is destroyed that it is done so appropriately and securely.** The school has procedures in place to destroy equipment and paper documents at the end of their life. IT equipment is sent to a registered WEEE recycling facility, with hard drives and data storage securely destroyed using certified and audited processes. All paper data is shredded and disposed of when it reaches the end of its retention period.

14. **Share personal information with others only when it is legally appropriate to do so.** All staff receive data protection training where they are instructed to follow this Data Protection Policy, the eSafety Policy and other relevant guides, to ensure that everyone is aware of their responsibilities for the security of the school's data.

15. **Comply with the duty to respond to requests for access to personal information (Subject Access Requests).** For a subject access request to be valid, it should be made in writing to the school, including via email or other electronic messaging, such as the contact

form on the school's website. Under the UK GDPR, individuals have the right to obtain confirmation of their data, the legal basis and category of data being processed, whether the data has been shared with other organisations and how long the data will be retained. Supplementary information should be included where relevant, such as the source of the data held, the right to rectification or erasure and the right to lodge a complaint with the Information Commissioners Office. Before complying with a Subject Access Request, the school will need to verify the identity of the person requesting the information and the lawfulness of providing that data.

16. **Ensure that all staff and governors are aware of and understand these policies and procedures, by providing regular training and resources.** Evidence will be retained of attendance, understanding and feedback from training sessions as an auditable resource, which will also feed into an ongoing training action plan. The school uses questionnaires to test current knowledge and skills of staff and Governors, which are used to inform additional training or resources to help staff recognise and meet their responsibilities.

17. **All staff are issued with an "IT and Data Protection Procedure Manual" to enhance and support the training schedule.** The manual outlines the procedures for staff to adhere to, in order to protect the school's IT estate and network as well as school data in all of its formats.

Photographs and videos of pupils

This section of the policy has been included to safeguard children and their identifiable data at all times and to ensure that they are only photographed or filmed with the full consent and knowledge of parents.

This will be administered in the following way:

- A Parentmail form is sent to all new Year R entrants and any family joining Hook Infants during the school year.
- Parents will be requested to electronically sign a consent in Parentmail. The consent record is retained in Parentmail for the duration of the child's attendance at the school. Details of all parent consent choices are compiled in a spreadsheet for day to day use.
- Occasionally we may have a parent who requests a paper consent form, which is then retained in the 'Permissions' folder in the office.
- Any parent who does not give consent for their child to be included in photographs or videos of school activities will be contacted by the Headteacher to establish if the child is to be removed from all photographic events or only specific ones.
- A list of children who are to be removed from named/all events will be kept in the school office.
- If possible and with parental consent, the staff will try to involve the children in all activities which may be filmed or photographed but without compromise to the anonymity of the children as requested.

Photographs and videos of staff

Staff are asked to sign a consent form to allow the school to use staff photographs for purposes without a legal basis, such as in the school newsletter or on the school website. At the beginning of each curriculum year all staff sign the same form and indicate which of the four uses (website, storage on IT systems, display boards and school publications) they give consent to.

The use of photos for school ID badges and other security matters do not require staff consent as these are processed under the school's legal obligations for site security, Safeguarding and child protection.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every three years. The policy review will be undertaken by the Data Protection Officer, Head teacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the school's Data Protection Officer and/or the school office for any data protection matters.

Data Protection Officer	Peter West Hook Infant School Church View, Hook Hampshire. RG27 9NR
Telephone:	01256 764489
Email:	dpo@hook-inf.hants.sch.uk

If you need to contact the school office if you have not received a response from the Data Protection Officer, or if you are not happy with your communication with them, please use the following contact details:

Come to reception at	Hook Infant School Church View, Hook Hampshire. RG27 9NR

or

Telephone:	01256 764489
Email:	office@hook-inf.hants.sch.uk

Approved by the Governing Body, Hook Infant School

Signed: Alison Collier

Chairman of Governing Body

Date: 25 January 2024

Review date: January 2025