# Itchen Abbas Primary School
# Data Protection Policy

The school collects and uses personal information (referred to in the UK General Data Protection Regulation (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 other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer, who may be contacted on 01962 779310.

The school issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, 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?**

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

**Data Protection Principles**

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

1. **Lawfulness, fairness and transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner. In order for personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the UK GDPR. These include (amongst other relevant conditions) where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority exercised by the school.

Where the special categories of personal data are processed, this shall include (amongst other relevant conditions) where processing is necessary for reasons of substantial public interest.

When processing personal data and special category data in the course of school business, the school will ensure that these requirements are met where relevant.

2. **Purpose limitation.** 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). The school will only process personal data for specific purposes and will notify those purposes to the data subject when it first collects the personal data or as soon as possible thereafter.

3. **Data minimisation**. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive. Personal data which is not necessary for the purpose for which it is obtained will not be collected.

4. **Accuracy.** Personal data shall be accurate and where necessary, kept up to date; Personal data should be reviewed and updated as necessary and should not be retained unless it is reasonable to assume that it is accurate. Individuals should notify the school of any changes in circumstances to enable records to be updated accordingly. The school will be responsible for ensuring that updating or records takes place where appropriate.

5. **Storage limitation.** 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. The school will not keep personal data for longer than is necessary for the purpose or purposes for which they were collected and will take reasonable steps to destroy or erase from its systems all data which is no longer required.

6. **Integrity and confidentiality**. Personal data shall be processed in a manner that ensures appropriate security of the personal data and which includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Duties**

Personal data shall not be transferred to a country or territory outside the UK and the European Union (EU)/European Economic Area (EEA), 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 in the UK GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the data controller.
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this.
- Inform individuals when their information is shared, and why and with whom unless the UK GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the UK and the EU/EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.
- Inform individuals of their data subject rights.
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests).
- Ensure that personal information is not transferred outside the UK and the EU/EEA without the appropriate safeguards.
- Ensure that all staff and governors are aware of and understand these policies and procedures.

**Retention and Disposal of Personal Data**

The school will dispose of personal data in a way which protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) as appropriate.

The school maintains a Retention Schedule that is specific and relevant to the specific types of information retained. The schedule outlines the appropriate periods for retention in each case.

**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.org.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 Data Protection Office, 01962 779310, who will also act as the contact point for any queries.

**Governors Review: July 2023**

**Next review: July 2026**

Last updated January 2021

# Appendix: Data protection detail

## 1. Computer-based information

### Data storage locations

- All *central shared data* is stored on local media within the locked IAPS computer cupboard
- The admin officer stores data on a password-protected Windows computer (in addition to the *central shared data* storage)
- The headteacher stores data on a password-protected Apple computer (in addition to the *central shared data* storage)
- Staff are permitted to store data on encrypted memory sticks for remote working
- Excepting the headteacher and the admin officer storage as described above, no members of staff store data other than in the *central shared data* storage facility or on encrypted memory sticks

### Central shared data types

*Central shared data* is divided into the following classes:

- *Open_access* data (**no** personal data present)
- *Staff_only* data (personal data may be present)
- *Archive* data (personal data may be present)
- *Individual folders - pupil* (**no** personal data present)
- *Individual folders - staff* members (personal data may be present)

### Computer access

- Three login types exist - *group logins*, *individual staff logins* and *pupil logins*
- *Individual staff logins* require a user id and password
- *Individual pupil logins* require only a user id
- All pupils, classroom assistants, admin officers, Headteacher and teachers have an appropriate individual login; other members of staff do not (e.g. caretakers, dinner ladies); neither do governors

- Two group logins exist: *staff* - reserved to classroom assistants, teachers, the Headteacher and admin officers (does requires a password); *pupil* – reserved to pupils (does not require a password)

## Data access

- Group logins do not allow any access to *central shared data*; they do permit use of a local account only on the logged-on machine
- All staff and pupils can read/write *open_access* data using their individual logins
- Only staff can read (but not write) *archive* data using their individual logins
- Only staff can read/write *staff_only* data using their individual logins
- Only the individual staff member can read/write their *individual staff* folder; no-one else has access
- All staff plus the individual pupil can read/write an *individual pupil* folder

## Wireless network access

- The wifi network is protected by WPA2 security and requires a password
- Connectivity to remote machines (including the internet) is enabled with the wifi password (connectivity but not necessarily data access)
- The wifi password is configured by IT on all IAPS machines - the password itself is kept secret
- Governors, on request, will be supplied with the necessary information for connectivity (but not access to local machines)

## Email accounts

- Two e-mail systems are in use in IAPS; one with addresses of the form of *****@itchenabbas.hants.gov.uk* is supplied by HCC and is only used by the Admin Officer and the Headteacher; the other with addresses of the form ****@itchenabbas.org.uk* is used for pupils, staff members and governors
- Both e-mail systems are password protected

## Data security requirements

- Staff members and governors must use their IAPS mail system for all school

business; personal e-mail accounts may not be used to communicate with parents, governors, other members of staff, or others on school business

- IAPS desktop computers and laptops, when used by staff, must be protected by a password-enabled screen saver when the staff member is not present
- IAPS iPads, when used by staff to access personal data, must have no such data accessible when the staff member is not present
- If personal data is removed from the school on a memory stick (or similar device) by a member of staff it must be encrypted and suitably protected against loss; such instances need to be approved in advance by the Data Protection Officer

## 2. Paper-based information

### Data storage locations

- The cupboards and desks of the Admin Officer and the Headteacher (personal data may be present)
- The PPA room (no personal data present)
- The computer cupboard (personal data may be present)

### Access

- The cupboards and desks of the Admin Officer and the Headteacher are secured with keys and only their owners have access. No documents are left unattended, accessible or visible
- The PPA room is not secured and is freely accessible

The computer cupboard is locked and only the IT consultant and the Data

Protection Officer have keys; other staff must request supervised access from the

Data Protection Officer