Howardian Primary School

Personal Data & Passwords Policy - 2025

Introduction - Personal Data and Sensitive Personal Data

The school and individuals may have access to a wide range of personal information and data, held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about children / young people, members of staff / volunteers and parents and carers eg. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records eg. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families

It is the responsibility of all staff and volunteers to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not have permission to access that data or does not need to have access to that data. Anyone who has access to personal data must know, understand and adhere to the schools data policy.

To clarify, sensitive personal data is defined as:

Information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

The General Data Protection Regulation (2018) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Responsibilities

The Headteacher, supported by the IT Manager, will keep up to date with current legislation and guidance and will carry out risk assessments.

All schools must register as a Data Controller on the Information Commissioner's Office (ICO) website. This notification should be reviewed on an annual basis to ensure that the school is still processing data in line with the purposes notified to the ICO.

Training & awareness

Staff and volunteers will receive GDPR training and will be made aware of their responsibilities, as described in this policy through;

- Induction training for new staff
- Meetings / briefings / training for staff / volunteers
- Day to day support and guidance from the Headteacher.

Risk Assessments

Information risk assessments will be carried out by staff / volunteers to establish key areas of the school where data might be at risk and how the risk could be reduced

Storing personal data

Personal data must be held securely on the school's premises or with the schools shared staff drives accessed through Hwb. This can only be accessed by those with permission to do so. Any personal data removed from the premises should have the appropriate level of protection to prevent loss of data. i.e encrypted laptops, password protected iPads etc

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required. Such data must be destroyed, rather than deleted and be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, and other (paper based) media must be shredded, incinerated or otherwise disintegrated. Should a 3rd party service be used, then a certificate of destruction should be obtained.

Password Security Policy - Introduction

The school will be responsible for ensuring that the technology is as safe and secure as is reasonably possible and that:

- users can only access data to which they have permission.
- access to personal data is securely controlled in line with the school's personal data policy.

Responsibilities

- The management of the password security policy will be the responsibility of the *IT Manager*.
- Each staff user should have their own password and be responsible for its security.
- *Passwords for new users, and replacement passwords for existing users will be allocated by the IT Manager.*
- *Staff users must not login other adults to the school system or Hwb using their login details & password. A separate 'generic' login exists for supply teachers and visitors to the school which gives them limited access to the school systems. (Username and password: Supply/Supply & visitor/visitor)*
- *Staff iPads, that have access to shared teacher drives or teacher emails etc, must be password protected.*
- *Staff Users must ensure they have logged out or locked a computer when they leave it unattended for any length of time.*
- *Staff users should periodically change their system password. (press ctrl - alt - delete when logged in at school).*
- *Personal devices that have access to online services (e.g Hwb email, Calendar or Drive) must be password protected.*

Training / Awareness

- It is essential that staff users should be made aware of the need for keeping passwords secure, not written down or shared with anyone else.
- Staff users will be made aware of the password policy:
    - - at induction
    - - through the IT Acceptable Use Agreement
- Pupils will be made aware of the password policy:
    - - when joining the school / informally through reminders from staff / volunteers.
    - - through the IT Acceptable Use Agreement.
    - - as part of the DCF cross curricular responsibility.