# Notting Hill Preparatory School

# 1.26 Information Security Policy

# (EYFS & KS1-3)

| | | | |
|---|---|---|---|
| Reviewer responsible: | **Bursar** | Date of last review: | **05/21** |
| Reviewed by: | NB | Date of next review: | **09/21** |

## INFORMATION SECURITY POLICY

### Introduction

Schools collect and process personal information to deliver educational services. This information is held about a variety of people and it is essential that the availability and confidentiality of accurate relevant information is maintained in a secure and legal environment. Notting Hill Preparatory School is committed to full compliance with its responsibilities under the Data Protection Act 1998 and General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). To actively demonstrate this, the School has issued a policy commitment which provides assurance to pupils, parents, governors and staff that sound and secure measures are in place to protect the confidentiality, integrity and availability of their information.

### Objective

The information security objective is to ensure that the school's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

### Policy

The purpose of this policy is to protect the school's information assets from all threats, whether internal or external, deliberate or accidental. The key aims of the policy are to ensure that:

- Information is protected from unauthorised access;
- Confidentiality of personal or sensitive information is assured.
- Integrity of information is maintained.
- Information is disposed of in a timely, appropriate and secure manner.
- Legislative requirements and school policy and practices are observed.
- Business continuity plans are produced, maintained and tested.
- Appropriate monitoring and reporting processes are put in place to act upon breaches of information security.

### Supporting Framework

In order to achieve this, the school will develop and maintain information security standards. Procedures, working practices and protocols will be developed to support this policy. Examples of measures to achieve the above are physical security, acceptable use policies, data storage and backup procedures, virus control, data protection impact assessment for all new software used and the use of passwords for access control.

### Data & Computer Security

NHP undertakes to ensure security of personal data by the following general methods:

- **Physical security**: Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear visitor badges whilst in the school and are, where appropriate, accompanied.
- **Logical security**: Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up regularly.
- **Procedural security**: All authorised staff are made aware of their Data Protection obligations and their knowledge updated as necessary. Confidential or sensitive computer printouts as well as source documents are shredded before disposal. Overall security of data is determined by the Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. Any queries or concerns about security of data in the school should, in the first instance, be referred to the Headmistress.
- **Working away from School**: Members of staff who work using equipment outside School and/or remove data from School must be aware of the additional risks to data security and take appropriate steps to mitigate them. No devices or data should be left in insecure locations. No member of staff is permitted to remove personal data or other confidential or sensitive data

from the school site, whether in paper or electronic form, without the prior consent of a member of the Senior Management Team. Staff must use outlook via Microsoft 365 for all email communications during directed working hours if they are working away from school. The use of personal email accounts are discouraged.

**Responsibilities**

The school's Bursar has direct responsibility for maintaining this policy and providing advice and guidance on its implementation. **All members of the school community have a role to play in information security. The secure handling of school data is everyone's responsibility – whether you are an employee, self-employed member of staff, volunteer, consultant, external contractor or software provider. Individual members of staff can be personally liable in law under the terms of the Data Protection Act and General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and may be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorized use or disclosure of their data. Failing to apply appropriate controls to protect this data could be considered to be gross misconduct and may lead to legal action or dismissal.**