DATA PROTECTION POLICY

Throughout this document we refer to Data Protection Legislation which means the Data Protection Act 2018 (DPA2018), the United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

Highfield Primary School will comply with the demands of the General Data Protection Regulation (GDPR) to be known as the Data Protection Act 2018.

Members of staff will gain familiarisation with the requirements of the GDPR either in a staff briefing or as part of their induction. This policy follows guidance issued by the Information Commissioner's Office (ICO) and the Department for Education (DfE).

The school is a Data Controller as data is processed that is the personal information of pupils, families, staff, visitors and other school users. The School is a Data Processor as it processes data on behalf of other public bodies such as the DfE.

Definitions

Data processing

The acquisition, storage, processing and transmission of data

Data subject

Any identifiable person whose data is processed

Consent

Must be freely given, specific and an unambiguous indication of the subject's wishes. It must be recorded and available to an audit. A person must be 13 years old in order to record their consent.

Cross-border processing

The GDPR covers all EU states and will remain part of UK law. Data cannot be stored beyond the EU and UK borders (the exact borders are those of the European Economic Area)

Sensitive data

The GDPR/ICO requires that particular care is taken with the following data

- Data regarding children
- Health (physical, mental, genetic)
- Ethnicity
- Religion
- Sexuality
- Performance management and trade union membership

Filing system

Any structured set of personal data, however stored in any format (physical or digital) that can be processed.

Personal data breach

A breach of data security leading to the accidental or unlawful destruction, loss, theft, alteration, unauthorised disclosure, destruction, sale or access to any processed data. Data subjects affected by a data breach must be informed of the breach within 72 hours. Breaches must be reported to the ICO within 72 hours.

Pseudonymisation

The act of making data anonymous. There must be security between pseudonymised data and any data that could re-identify a person.

Password protection

The act of 'locking' a device or document. The information remains readable beyond the password.

Encryption

The act of encoding all the information beyond a password or code.

Legal basis

DATA PROTECTION POLICY

The school decides, and registers with the ICO, upon which legal basis it processes data. As a public body with set duties the school uses the following bases for processing and controlling data

Legal basis: Public Task

- Admissions
- Attendance
- Assessment
- Pupil and staff welfare
- Safe recruitment
- Staff training
- Performance Management

Legal basis: Consent

- Various uses of photographs and moving images
- Trade union membership
- Staff ethnicity, religion and health data (Note the Staff Privacy Statement)
- The use of data to promote the social life of the school community

Legal basis: Contract

- When processing is required to carry out the performance of a contract

Personal data

Anything that might lead to the identification of a person: name, number, characteristics, photograph, correspondence.

Data portability, data subject access request

Data subjects (or a child's parents) may request access to a copy of all their data. The school has established an efficient means of accomplishing this task which may not carry a charge and will be completed within 15 working days. Data subjects may request that data is brought up-to-date or made more accurate.

Principles

- Personal data must be processed lawfully, fairly and transparently
- Personal data can only be collected for specific, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to what is necessary for processing
- Personal data must be accurate and kept up-to-date
- Personal data may identify the data subject only as long as is necessary for processing
- Personal data must be processed in a manner that ensures its security
- Any breaches in data security must be reported to the ICO within 72 hours
- The school must report any breaches caused by third parties who have access to school users' data within 72 hours.
- The school must inform any data subject (person identified in data) where a data breach may have led to the unauthorised access to their personal information

Roles and Responsibilities

The school's Privacy Statements set out in detail how the school will maintain the security of school users' data. The Acceptable Use Policies set out the duties of the staff and other school users in supporting data security. Within school the security of data is coordinated by the Headteacher.
The school has appointed a Data Protection Officer who has responsibility for overseeing the implementation of this policy and all GDPR related documents. The DPO will monitor compliance, report to the school leadership and support the school with updates and interpretations as the GDPR develops. The DPO will liaise between the school and the ICO and must be informed as soon as is practicable of any personal data security breach. The DPO will support the school in its communication with schools users (pupils, families, parents, governors, contractors and visitors) about the school's GDPR procedures. This will include the drafting of privacy statements, acceptable use policies and data subjects rights. Data subject requests should be made in writing to the DPO.

DATA PROTECTION POLICY

Children below the age of 13 do not have the right to make a subject access request, so requests must be made by parents. The school may take into account the views of a pupil.
The school's DPO is:

The DPO Centre Ltd., 50 Liverpool Street, London EC2M 7PY

Advice Line number 0203 797 6340

Sharing Data

Personal data may be shared with third parties to

- Protect the vital interests of a child
- Protect the vital interests of a member of staff
- To prevent or support the detection of fraud or other legal proceedings
- When required to do so by HMRC

Photographs and moving images

Consent is requested from parents. Letters requesting consent outline the choices that pupils may make for the use of their images.
The school may seek consent to use photographs for the following purposes:

- To support school user welfare (identity and security)
- To celebrate achievement within the classroom
- To celebrate achievement within the school
- To celebrate achievement in the printed press
- To celebrate achievement online

The school's specific data security measures - data protection by design

A. All IT systems - mobile devices, laptops, tablets, mobile phones and any device capable of processing data, will be password protected.
B. All IT systems will be kept securely; desktop computers and portable devices will be sited/stored in secure places.
C. Staff are expected to ensure the safety of their allocated school devices: devices may not be left unattended in cars at any time and they must be kept out of sight if taken home.
D. All passwords must be 'strong;
E. No passwords will be shared;
F. The school will devise granulated levels of access as appropriate to staff responsibilities for access to personal data.
G. All emails containing personal data will use school systems and be encrypted school email accounts to be used
H. All delated data will be deleted in a secure manner: physical data will be shredded and digital data will fully deleted with trash / junk emptied regularly.
I. Only data that is necessary for the effective performance of the school will be processed.
J. Physical data will be kept securely, having regard to the sensitivity of the data and the vulnerability of the data subject e.g. medical data will be accessible to those who need to support a school user's needs, but not to others.
K. All school users will handle personal data with care: papers must not be left where others can see them.
L. Personally owned devices will not be used for the storage of school personal data.

Data breaches

All staff must report to the head teacher any suspected data breaches (the loss, theft, unauthorised access to data etc.) immediately. It will be for them to decide (following consultation and advice

from the DPO) whether the suspected data breach warrants reporting to the ICO. NB a data breach would include the accidental sharing of personal data via a wrongly addressed email.

Training

All staff will receive basic training in the requirements of the GDPR.

Monitoring

The DPO will lead the formal monitoring of the school's compliance with the GDPR. Every member of staff and governor shares a responsibility to monitor compliance and to report any suspected failures to comply.

Policy approved by the Governing Body

Date approved 23th November 2021_____

Date for review November 2023_____