Data Protection Policy

Reviewed– Annually	**F & P Committee**
Reviewed on	**Signed**

1. Rationale:
As a school we handle increasing amounts of personal information and have a statutory requirement to comply with The Data Protection Act 1998("DPA") and the GDPR regulations from May 2018. Schools should have clear policies and procedures for dealing with personal information, and be registered with the Information Commissioner's Office ("ICO"). Schools should have systems in place to reduce the chances of a loss of personal information, otherwise known as a data breach which could occur as a result of theft, loss, accidental disclosure, equipment failure or hacking.

2. Aims and Objectives:
The aims of our Data Protection Policy encompass the following:
Morality

- To foster an ethos of trust within the school where all who handle personal data do so within the framework of the law.
- To ensure that confidentiality is a whole school issue and that in lessons ground rules are set for the protection of all.
- To ensure that if there are child protection issues then the correct procedure is followed as outlined in the school's Child Protection policy.

Communication

- To ensure that staff, parents and pupils are aware of the school's Data Protection Policy and procedures and how personal data should be processed, stored, archived and deleted/destroyed
- To provide consistent messages in school about handling information about children, staff and families once it has been received.
- To ensure that children/parents know that school staff cannot offer unconditional confidentiality.

Cooperation

- To reassure children that their best interest will be maintained.
- To ensure that staff and parents have a right of access to all records held on them or their child(ren), except where the sharing of these could endanger the child.

Respect

- To protect personal data at all times and to give all school staff clear, unambiguous guidance as to their legal and professional roles and to ensure good practice throughout the school which is understood by children, parents /carers and staff.
- To ensure that there is equality of provision and access for all including rigorous monitoring of cultural, gender and special educational needs.

3. Data Protection Principles
The Data Protection Act 1998 (DPA) and the General Data Protection Regulations (GDPR) establish and recognise eight principles that must be adhered to by the school at all times. These are that:

1. Personal data shall be processed fairly and lawfully;

2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

4. Data Types

Not all data needs to be protected to the same standards, the more sensitive or potentially damaging the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In the Monkton Park Primary School environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar approach takes place with managing school data. The DPA defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a "Potential Data Breach" which could result in legal action against the school. The loss of sensitive personal data is considered much more seriously and the
sanctions may well be more punitive.

4.1 Personal data

Monkton Park Primary School has access to a wide range of personal information and data. This data may be held in a 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 includes:

- Personal information about members of the school community – including pupils, members of staff and parents/carers eg names, addresses, contact details, legal guardianship contact details, disciplinary records.
- Curricular/academic data eg class lists, pupil progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records, disciplinary records and references

- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

4.2 Sensitive Personal data
Sensitive personal data is defined as information that relates to the following eight categories:
race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life and criminal offences, criminal proceedings.
It requires a greater degree of protection and in Monkton Park Primary School will include:-

- Staff Trade Union details
- Information on the racial or ethnic origin of a child or member of staff
- Information about the sexuality of a child, his or her family or a member of staff
- Medical information about a child or member of staff
- Information relating to any criminal offence of a child, family member or member of staff.

Note *– On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate written permission should be sought from the parents / carers before posting information more widely, for instance in the staff room.*

4.3 Other types of Data not covered by the Data Protection act or GDPR.
This is data that does not identify a living individual and therefore is not covered by the remit of the DPA this may fall under other access to information procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual.
Responsibilities
The Headteacher and Governing Body are responsible for Data Protection. At Monkton Park School we have two key roles within the school to manage data. The first of these positions is held by Linda Paynter as the Data Protection Officer (DPO) and the second position is held by Sarah Quarrell as Data Protection Controller (DPC). These two post holders will ensure that the school manages data within the law and responds appropriately if there are any data breaches.

4.4 Risk Management – Roles
DPO
The DPO's minimum tasks are defined in Article 39 of the GDPR and their responsibilities include, but are not limited to:

- Educating the school and its staff on important compliance requirements

- Training staff involved in data processing.
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the school and GDPR Supervisory Authorities.
- Monitoring performance and providing advice on the impact of data protection efforts.
- Maintaining comprehensive records of all data processing activities.
- Interconnecting with data subjects or parents to inform them about: how their data is being used; their rights to have their, or their child's personal data erased; the measures in place to protect their, or their child's, personal information.

In Monkton Park Primary School we have a DPO who has an understanding of data protection from an educational perspective but who is objective and impartial in relation to our school's organisation around data protection.

DPC

The DPC is involved with the ongoing day to day operations within the school. Their responsibilities include, but are not limited to ensuring that the school is compliant with the following rules:

- That personal data is processed legally and fairly
- The data the school collects is collected for legitimate purposes and used accordingly
- The data collected by the school is adequate and relevant and is not be excessive in relation to the reason it has been collected (or processed)
- Data collected by the school is updated regularly and is accurate
- That any personal data held by the school is rectified, removed and is blocked if incorrect
- Anything that identifies individuals must not be kept too long
- Anything personal must be protected against accidental, unlawful destruction, alteration and disclosure; especially when it involves processing data over networks

Data controllers must implement appropriate security measures and these measures need to have the appropriate level of protection for the data stored and processed.

If an individual (staff member, parent, pupil) believes that their data has been compromised they can send a complaint to the 'data controller', if they feel that the schools handling of their complaint is not to their satisfaction they can then file a complaint with the national supervisory data protection authority.

Within the above role the DPC also:

- Keeps a log of data breeches and talks to staff member breeching so that they can put things right.
- Reviews the log on a regular basis. Their responsibility is to identify if it is a conduct or capability action if things do not change. If this becomes serious it is reported to the DPO and evidence is then prepared to submit to the ICO
- The DPC will meet with the DPO on a regular basis.

In Monkton Park Primary School we have a DPC who has an understanding of data protection who works within our organisation.

4.5 Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

5 Legal Requirements

5.1 Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner and is responsible for its own registration.

5.2 Information for Data Subjects (Parents, Staff)

In order to comply with the fair processing requirements of the DPA, the school will inform parents/carers of all pupils and staff of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties eg LA, DfE, etc to whom it may be passed. The privacy notice is made available to parents/carers on the school website and was initially signposted/linked via a letter at the onset of GDPR.

6 Transporting, Storing and Deleting Personal Data

The policy and processes of the school comply with the guidance issued by the ICO

6.1 Information Security - Storage and Access to Data

6.1.1 Technical Requirements

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to

protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.
- The school has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

6.1.2 Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected,
- The device must be password protected
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

6.1.3 Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared.

6.1.4 Photographs and Images

- Images of pupils will only be processed and transported by use of encrypted devices and permission for this will be obtained in a consent form.
- Images will be protected and stored in a secure area.

6.1.5 Cloud Based Storage

- The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote/cloud based data services providers to protect the data.

6.2 Third Party data transfers

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

6.3 Retention of Data

The school will keep some forms of information for longer than others. Information will not be kept indefinitely, unless there are specific requirements. In line with principle 5 of the data protection act information should not be kept longer than is necessary. The retention schedule gives a breakdown of timescales for the retention of various types of information.

When data is no longer required it will be appropriately destroyed. Personal data that is no longer required will be destroyed.

6.4 Systems to protect data

6.4.1 Paper Based Systems

- All paper based official or sensitive (or higher) material must be held in lockable storage, whether on or off site.

6.4.2 School Websites

- Uploads to the school website will be checked prior to publication ensure that personal data will not be accidently disclosed and that images uploaded only show pupils where prior permission has been obtained

6.4.3 E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

E-mails containing sensitive information should be encrypted, for example by attaching the sensitive information as a password protected word document. The recipient will then need to contact the school for access to a one-off password

6.5 Disposing of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required as specified in the IRMS Information Management Toolkit for Schools The disposal of personal data, in either paper or electronic form, will be conducted in a way that makes reconstruction highly unlikely. Electronic files will be securely overwritten, in accordance with government guidance, and other media will be shredded, incinerated or otherwise disintegrated for data.

7. Subject Access Requests

Parents/carers of all pupils and staff have the right to obtain confirmation from the school as to whether or not personal data concerning a child or them personally is being processed, and, where this is the case, access to this personal data and information.

The school will provide a copy of the personal data. Where the request is by electronic means, and unless otherwise requested by the subject, the information will be provided in a commonly used electronic form.

The right to obtain a copy of personal information will be completed within one month (where reasonable). This is to allow the school to process the request without adversely affecting the rights and freedoms of others.
The school does however have the right to refuse or charge for requests that are manifestly unfounded or excessive. Where the school exercises this right the school will inform the subject of their right to complain to the supervisory authority.

8. Data Breach – Procedures
SEE DATA BREACH POLICY

9. Training
The school recognises that many data protection failures are caused by ignorance and anything that promotes awareness is to be recommended. Mistakes can often be prevented by being aware that a potential problem exists and knowing who can give more detailed advice. To this end all staff will receive written and practical guidance on confidentiality of personal information and how this links to written policies.
Practical guidance will be provided through school CPD every three years (or earlier as required) and on an annual basis through the school's adult code of conduct. Both the training and codes of conduct will be signed for by the staff member/adult to confirm that they understand their responsibilities in relation to data protection

10. Associated Policies and Procedures:
Data Breach Policy
Privacy Notice for Staff
Privacy Notice for Pupils/Parents
Consent form (Data and Images)

11. Policy Review Reviewing:
This policy will be reviewed annually.

Glossary
Data Protection Act 1998: All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.
ICO The Information Commissioner's office. This is a government body that regulates the Data Protection Act.
The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England: General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media: General information note from the Information Commissioner on publication of examination results.
Education Act 1996: Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005: Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972: Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998: Retention of school admission and exclusion appeal papers and other pupil records.