Moorside High School

Data Protection Policy

Date Reviewed: ……May 2017……..
Date of Next Review: ……May 2018……..
Reviewed by: ……Health & Safety Committee

May 2017

This data protection policy will be reviewed annually by the personnel committee of the Governing Body.

Date of next review: Summer 2018

Introduction

Moorside High School recognises and accepts its responsibility as set out in the Data Protection Act 1998 and sub-legislation contained therein. The school, as a data controller, will take all reasonable steps to meet this responsibility and to promote good practice in handling and use of personal information. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

1. Fairly and lawfully processed.
2. Processed for limited purposes.
3. Adequate, relevant and not excessive.
4. Accurate.
5. Kept no longer that is necessary.
6. Processed in accordance with the data subject's right.
7. Secure.
8. Only transferred to others with adequate protection.

This policy statement applies to all Moorside High Governors, employees and individuals about whom Moorside processes personal information.

It is the responsibility of all members of school community 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 who does not need to have access to that data.

Any loss of personal data can have serious effects for individuals and or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and/or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

The Data Protection Act 1998 lays down a set of rules for processing personal data (both structured manual and digital records). It provides individuals (data subjects) with right of access and security and requires users of data to be open about how it is used and to follow "good information handling principles".

Policy Statements

Moorside High will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. It will not retain personal data for longer than is necessary to ensure compliance with legislation, and any other statutory requirements.
Every effort will be made to ensure that the information is accurate, up to date and that inaccuracies are corrected without delay.

All personal data will be fairly obtained and lawfully processed in accordance with the "Privacy Notice".

Responsibilities

Moorside's data protection officer and the person with specific responsibility for data protection is the Office Manager. They will keep up to date with current legislation and guidance and will:

1. Notify the school's processing of personal data with the Information Commissioner's Office.
2. Observe the eight data protection principles.
3. Make sure that everyone managing and handling personal information understands that they are contractually responsible for the following good data protection practice.
4. Ensure that the rights of people about whom information is held can be fully exercised under the 1998 Act.

Everyone at Moorside High has responsibility of handling protected or sensitive data 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 with their role a Governor.

Personal Data

The school and individuals will have access to a wide range of personal data. The data may be held electronically 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:

1. Personal information about members of the school community including students, staff, parents and carers for eg. Names and addresses, contact detail, legal guardianship, health records and disciplinary records.
2. Curricular/academic data eg. Class lists, student progress records, reports and references.
3. Professional records eg. Employment history, taxation and national insurance records, appraisal records and references.
4. Any other information that might be disclosed to parents/carers or by other agencies working with families or members of staff.

Moorside will also, on occasions, make use of personal data relating to staff, pupils, their parents or guardians in the following ways:

Make use of photographic images of staff and pupils in Moorside High publications and on the Moorside High School website; for fundraising, marketing or promotional purposes. These individuals have a right to limit or object to any such use by notifying the school in writing. However the school will not publish photographs of individuals with their names on school website/newsletter or other media without the express agreement of the appropriate individual, parents or guardians as applicable.

Subject Access

The Data Protection Act extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

1. Requests from pupils will be processed as any subject request.
2. Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
3. Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing Subject Access Requests

Requests for access must be in writing.

Moorside High, in general, only discloses data about individuals with their consent. However there are circumstances under which Moorside may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the School to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosers, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the School.
- Only authorised and trained staffare allowed to make external disclosures of personal data. Data used within the School by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the School who needs to know the information in order to do their work. The School will not disclose anything on pupils' records which is likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggestions that they are, or have been, either the subject of or at risk of child abuse.

Information to parents/carers – "The Privacy Notice"

Under the "Fair Processing" requirements in the Data Protection Act, the School will inform parents/carers of all pupils/students of the data they hold on students, the purposes for which the data is held and the third parties (e.g. LA, DfE etc) to whom it may be passed. This privacy notice will be available on the School website.

Training & Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities in managing and handling personal information, as described in this policy through:

- Induction training for new staff.
- Staff meetings/briefings/Inset.
- Day to day support and guidance from information controllers.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged- off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Secure Storage of and Access to Data

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.

All users will be given secure user names and strong passwords which must be changed regularly as per the School's password security policy. User names and passwords must never be shared.

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 a very short time periods) and set to auto lock if not used for five minutes.

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). Private equipment (i.e. owned by the users) must not be used.

When personal data can only be stored on a portable computer system, USB stick or any other removable media:

- The data must be encrypted or password protected.
- The device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected).
- The device must offer approved virus checking software.
- 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.

The School has clear policy and procedures for the automatic backing up, accessing and restoring all data held on School systems, including off-site backups.

All paper based Protected and Restricted (or higher) material must be held in lockable storage.

Secure transfer of data and access out of School

The School recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the School or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside the School premises (for example, by a teacher or student working from their home or a contractor) they must have a secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of data

The School will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.