Policy No.: 7

Policy: Data Protection

Review Date: June 2017

Policy Name: Data Protection

Nominated Lead Member of Staff: ICT Manager

Review Cycle: 2 Years

Authorisation: Governing Body

Review Date: June 2017

Data Protection Policy

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Headteacher and Governors of this School intent to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Enquiries

Information about the school's Data Protection Policy can be viewed on the school website. Hard copies are available upon request. General information about the Data Protection Act can be obtained from the governmental website https://www.gov.uk/data-protection

Fair obtaining and processing

Matthew Moss High School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subject's right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

Terminology

"Processing" - means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
"Data subject" - means an individual who is the subject of personal data or the person to whom the information relates.
"Personal data" - means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
"Parent" - has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

Data integrity

The school undertakes to ensure data integrity by the following methods:

Data accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their computer record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data adequacy and relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. Annually, parents are asked to update the contact information held by the school for accuracy. Also, admin staff check any information held by the school against parental consent forms for trips.

Length of time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of admin staff and the Senior Leadership Team to ensure that obsolete data is properly erased.

Subject access

The Data Protection Acts extend 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 learner, the school's policy is that:

• Requests from learners will be processed as any subject access request as outlined below and the copy will be given directly to the learner, unless it is clear that the learner does not understand the nature of the request.
• Requests from learners who do not appear to understand the nature of the request will be referred to their parents or carers.
• Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing subject access requests

Requests for access must be made in writing.

Learners, parents or staff may ask for a Data Subject Access Request form, available from the School. The form is also available on the school website. Completed forms should be addressed to the Headteacher. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (eg Learner Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Learner Information) Regulations.

Authorised disclosures

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

• Learner data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
• Learner data disclosed to authorised recipients in respect of their child's health, safety and welfare.

• Learner 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 eg in respect of payroll and administrative matters.
• Unavoidable disclosures, 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. Officers and IT personnel working on behalf of the LEA are contractually bound not to disclose personal data.

Only authorised and trained staff are 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 need to know the information in order to do their work. The school will not disclose anything on learners' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.
An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

Data and computer security

Matthew Moss High School undertakes to ensure security of personal data.

Physical security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the server room, which has door access restricted and monitored. Disks, tapes and printouts containing personal information are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification 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 computer files. This access is restricted via the use of Access Control Lists and can be managed on a per user or group basis. Password changes are enforced every 90 days and password complexity rules are enforced to prevent 'brute force' access to passwords. All computer files are backed up (ie security copies are taken) regularly according to a schedule which grants access to historical data going back 12 months. Any important data that is required for longer than this period is archived to optical media and stored securely. No data is taken off-site but in order to provide security of data in the event of fire, backup tapes are held at the opposite end of the school from the server room in a fireproof room.

Procedural security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the Headteacher/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 ICT Systems Manager.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from the ICT Systems Manager

Associated Policies:
All areas of school policy

Appendix 1

Schools Privacy Notice – 2014-2015

Data Protection Act 1998: How we use your information

We, **Matthew Moss High School**, are a data controller for the purposes of the Data Protection Act. We collect personal information from you and may receive information about your child from their previous school and the Learning Records Service. We hold this personal data to:

- Support their learning
- Monitor and report on their progress
- Provide appropriate pastoral care; and
- Assess the quality of our services

Information about our pupils that we hold will include their contact details, SAT assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information. For learners enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.

We are required by law to pass some information that we hold about pupils and parents to the Local Authority and the Department for Education (DfE). The Local Authority may occasionally be required to share your personal and sensitive information with other government and/or partner agencies. The Local Authority will only share data when there is a statutory duty or legal requirement to do so, for example, where the Local Authority is required to provide a programme of assistance. Any data that the LA share with the government and/or partner agencies will be strictly assessed and the Local Authority will ensure that the requirements of the Data Protection Act 1998 are compiled with.

In addition once our leaners reach the age of 13 or over, the law requires us to pass on certain information about them to providers of youth support services in our area who have responsibilities in relation to the education or training of 13-19 year olds. We provide them with the learners' names and addresses, dates of birth, name(s)/address(es) of their parent(s)/guardian(s) and any other information relevant to their role. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them.

A parent/guardian can ask that no information apart from their child's name, address and date of birth be passed to the support service by informing **Mrs Karen Neville (Business Manager).** This right is transferred to your child once he/she reaches the age 16. For more information about services for young people, please go to the National Careers Service page at
https://nationalcareersservice.direct.gov.uk/aboutus/pages/default.aspx

We will not give information about you to anyone without your consent unless the law and our policies allow us to.

If you want to receive a copy of the information about you that we hold or share, please contact **Mrs Karen Neville.**

If you need more information about how our local authority and DfE store and use your information, please visit:

- Information Governance Unit, Rochdale Council, Number One Riverside, Floor 2, Smith Street, Rochdale, OL16 1XU
  Email: foi@rochdale.gov.ukmailto:foi@rochdale.gov.uk
  Telephone: 01706 925505
  Email:
  http://www.rochdale.gov.uk/council_and_democracy/data_protection_and_foi/pupil_data.as.px

  or

- the DfE website at
  https://www.gov.uk/data-protection-how-we-collect-and-share-research-datahttps://www.gov.uk/data-protection-how-we-collect-and-share-research-data
  Public Communications Unit, Department for Education, Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
  Email:
  http://www.education.gov.uk/help/contactushttp://www.education.gov.uk/help/contactus
  Telephone: 0370 000 2288