The Maltby Learning Trust

# MLT Data Protection Policy

| | |
|---|---|
| Date Last Reviewed: | September 2016 |
| Reviewed by: | ICT Team Leader |
| Approved by: | MLT Board |
| Next Review Due: | September 2018 |

Maltby Learning Trust

## STATEMENT OF INTENT

Maltby Learning Trust is required to keep and process certain information about its staff and students in accordance with its legal obligations under the Data Protection Act 1998. The Trust may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the LA, other schools and educational bodies, and other third parties.

This policy is in place to ensure all staff and governors are aware of their responsibilities under the Data Protection Act and outlines how Maltby Learning Trust complies with the following core principles of the Act:

- Data must be processed fairly and lawfully.
- Data must only be acquired for one or more lawful purposes and should not be processed for other reasons.
- Data must be adequate, relevant and not excessive.
- Data must be kept accurate and up-to-date.
- Data must not be kept for longer than is necessary.
- Data must be processed in accordance with the data subject's rights.
- Appropriate measures must be taken to prevent unauthorised or unlawful access to the data and against loss, destruction or damage to data.
- Data must not be transferred to a country or territory unless it ensures an adequate level of protection for the rights of the subject.

Organisational methods for keeping data secure are imperative, and Maltby Learning Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

## 1. DATA CONTROLLER

1.1. The Maltby Learning Trust as the corporate body, is the data controller.
1.2. The CEO of Maltby Learning Trust therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.
1.3. The Director of Business and Finance/CFO will deal with the day-to-day matters relating to data protection.
1.4. The Director of Business and Finance/CFO is responsible for processing personal information on the Trust's behalf.
1.5. On occasion, personal information may be processed by Maltby Learning Trust. By involving another organisation in the data processing, the Trust accepts and mitigates against an increase in certain risks, for example, fraudulent activities.

## 2. FAIR PROCESSING

2.1 Maltby Learning Trust recognises that its staff and students need to know what the Trust does with the information it holds about them.
2.2 A copy of this Data Protection Policy is available for viewing on the Maltby Learning Trusts website.
2.3 Maltby Learning Trust issues a general privacy notice, detailing the purposes for which personal data collected by the Trust will be used, before obtaining or responding with a request for any personal information.
2.4 If personal details are being recorded for a specific purpose, a specific privacy notice may be issued.
2.5 The general privacy notice is also published on the Maltby Learning Trust's website.
2.6 Personal information is classified as 'Confidential/Restricted data' and is only made available to staff and governors who need that particular information to do their jobs, and at the time that it is needed.
2.7 All staff members, including members of the governing body will receive DP guidance in respect of their responsibilities.
2.8 The guidance will be reinforced at regular intervals throughout their employment/term as governor, e.g. on inset days or via email communication.
2.9 Staff members and parents are responsible for checking that any information that they provide to the Trust in connection with their employment or in regard to a registered student is accurate and up-to-date.
2.10 The Trust cannot be held accountable for any errors unless the employee or parent has informed the Trust in writing about such changes.
2.11 The Director of Business and Finance/CFO is responsible for monitoring fair processing controls on a regular basis.

## 3 DATA SECURITY

3.1 Confidential paper records are kept in a locked secure area, with restricted access. Information should not be left on office desks at the end of the day.
3.2 Confidential paper records should not be left unattended or in clear view anywhere with general access.
3.3 Confidential information should not be left open and visible of workstations; staff should ensure that the screen is locked if leaving the workstation unattended.

3.4 Where data is saved on removable storage or a portable device, the device must be encrypted and kept in a locked secure area when not in use.
3.5 Memory sticks should not be used to hold personal information unless they are password-protected and fully encrypted.
3.6 All electronic devices must be password-protected to protect the information on the device in case of theft.
3.7 Where possible, the Trust enables electronic devices to allow the remote blocking/deletion of data in case of theft.
3.8 Staff and governors should not store Academy data on their electronic personal devices.
3.9 All necessary staff are provided with their own secure login and password.
3.10 Emails containing sensitive or confidential information should be password-protected if there are insecure servers between the sender and the recipient.
3.11 Circular emails to parents should be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
3.12 When sending confidential information by email or fax, staff must check that the recipient is the correct addressee before sending.
3.13 Maltby Learning Trust uses encrypted zip files for secure sending system.
3.14 Where personal information that could be considered private or confidential is taken off the school premises, either in electronic or paper format, staff must take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises must accept full responsibility for the security of the data.
3.15 Before sharing data, all staff must ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

3.16 The physical security of the school buildings and storage systems, and access to them, is reviewed annually. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
3.17 Maltby Learning Trust takes its duties under the Data Protection Act seriously and any unauthorised disclosure may result in disciplinary action being taken.

## 4. SUBJECT CONSENT

4.1 Maltby Learning Trust understands that subjects have certain legal rights to their personal data, which will be respected.
4.2 The Trust will not process personal data without the consent of the subject, although the processing of data will sometimes be necessary for:

- The performance of a contract to which the subject is party to, or the steps taken with a view to entering a contract.
- Compliance with a legal obligation to which the Trust is subject.
- The administration of justice, legal functions of persons or departments, or functions of a public nature exercised in the public interest.
- The purposes of legitimate interests of the Trust, unless the decision prejudices the rights, freedoms or legitimate interests of the subject.

4.3 Staff members of the Trust will be working in close contact with children. Enhanced Disclosure and Barring Service (DBS) checks will therefore be made a condition of employment in order to ensure that potential employees do not pose a threat or danger.

4.4 Sensitive data, including: information relating to a subject's racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health; their sex life; or the commission of any offence, can only be processed with the explicit consent of the subject.

4.5 Sensitive data will only be processed if:

- It is necessary to protect the subject's vital interests.
- It is carried out in the course of legitimate activities by a not-for-profit body or association with appropriate safeguards.
- It is necessary for the administration of justice or other legal purposes.
- It has been ordered by the Secretary of State.
- It is necessary to prevent fraud.
- It is necessary for medical purposes.
- It is necessary for equality reasons.
- It was made public deliberately by the data subject.

## 5. RIGHTS TO ACCESS INFORMATION

5.1 All staff members, parents of registered students and other users are entitled to:

- Know what information the Trust holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to keep it up-to-date.
- Understand what the Trust is doing to comply with its obligations under the Data Protection Act.

5.2 All staff members, parents of registered students and other users have the right, under the Data Protection Act, to access certain personal data being held about them or their child.

5.3 Personal information can be shared with students (from age 13) once they are old enough, although this information can still be shared with parents/carers.

5.4 Students old enough to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

5.5 The Trust aims to comply with requests for access to personal information as quickly as possible, but will ensure that it meets its duty under the Data Protection Act to provide it within 40 working days.

5.6 Maltby Learning Trust will comply with its obligations under the Data Protection Act to provide subjects access to personal information.

5.7 All subject access requests must be kept in a log that requires formal consideration.

5.8 The Trust may charge a fee of £10 or more on each occasion that access is requested.

5.9 The Trust is not obliged to provide unstructured personal data if the administrative cost is deemed to exceed the limit of £450 as contained in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

5.10 Maltby Learning Trust is not obliged to supply access to information unless it has received:

- A request in writing.
- The fee required.

## 6. PUBLICATION OF INFORMATION

6.1 Maltby Learning Trust will publish a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures.
- Minutes of meetings.
- Annual reports.
- Financial information.

6.2 Classes of information specified in the publication scheme will be made available quickly and easily on request.

6.3 Maltby Learning Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

6.4 When uploading information to the school website, staff must be considerate of any metadata or deletions which could be accessed in documents and images on the site.

## 7. CCTV AND PHOTOGRAPHY

7.1 Maltby Learning Trust understands that recording images of identifiable individuals constitutes processing personal information, so must be done in line with data protection principles.

7.2 Maltby Learning Trust notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards.

7.3 Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

7.4 Maltby Learning Trust keeps CCTV footage for a maximum period of 21 days for security purposes. The Director of Business and Finance/CFO is responsible for keeping the records secure and allowing access.

7.5 The Trust will always indicate its intentions for taking photographs of students and retrieve permission before publishing them.

7.6 If the Trust wishes to use images/video footage of students in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent/guardian of the student.

7.7 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the Data Protection Act.

## 8. DATA RETENTION

8.1 The Data Protection Act states that data should not be kept for longer than is necessary.

8.2 In the case of Maltby Learning Trust unrequired data will be deleted as soon as practicable.

8.3 Some educational records relating to a former student or employee of the Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

8.4 Records of Enhanced DBS checks will be destroyed immediately, although the date that the check was made will be retained in the Trust`s file.

8.5 Paper documents must be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

## 9. CHALLENGES AND COMPENSATION

9.1 Maltby Learning Trust understands that staff members and the parents of registered students have the right to prevent the processing of personal data if it is likely to cause damage or distress.

9.2 Individuals with concerns related to the processing of personal data should provide the Director of Business and Finance/CFO with written notice.

9.3 If the Director of Business and Finance/CFO receives a written notice asking them to cease or not to begin processing specified data, they must reply in writing within 21 days detailing:

- Their compliance or their intent to comply; or
- Their reasons for considering the subject's written notice unjustified and the extent to which they have complied, or intend to comply, with the request.

9.4 Data subjects reserve the right to take their concerns to a court of law and will be entitled to compensation if it is judged that the Trust contravened the provisions of the Data Protection Act.

9.5 It is the individual's own responsibility to take action for compensation if loss of personal data causes them damage.

9.6 The Trust will immediately rectify, block, erase or destroy any data that a court of law judges to have contravened the requirements of the Data Protection Act.

## 10. SUBJECT ACCESS REQUESTS

### DEFINITION

A subject access request (SAR) is created by section 7 of the Data Protection Act 1998. All requests must be made in writing to the CEO or respective Academy Principal, who have a legal requirement to respond to the requester within 15 school days, if the information requested is regarding an educational record. If the data being requested is not related to this, the response must be within 40 calendar days.

Dependent on the nature of the SAR, the requester may be required to pay a fee. An individual who makes a written request is entitled to be:

- Informed whether any personal data is being processed.
- Given a description of the personal data.
- Told whether the information will be given to any other organisations or people.
- Given details of the source of the data (where this is available).
- Given a copy of the information.

## INDIVIDUAL'S RIGHT TO REQUEST

It is the child who has right of access to the information held about them; however, in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

The Trust has the responsibility of considering whether a child is mature enough to understand their rights. If you are confident that the child is mature enough, then it is your duty to respond to the child rather than the parent/carer, or to ask for the child's permission to disclose the information. (ICO, p.50)

When considering cases, we take into account the following:

- The nature of the personal data
- The child's level of maturity and their ability to make decisions
- Any court orders relating to parental access or responsibility that may apply
- Any duty of confidence owed to the child
- Any consequences of allowing those with parental responsibility access to the child's information (this is particularly important if there have been allegations of abuse or ill treatment)
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information
- Any views the child or young person has on whether their parents should have access to information about them
- What they can request
- Parents of children at a maintained school have the right to access their child's educational record. This includes information that is processed by the governing body or that is sourced from any of the following:
- Member of staff
- LA employee
- The student
- The parent
- Educational psychologist

For students at an academy, free or independent school, there is no equivalent legal right for parents/carers to access their child's educational records. It is at the school's discretion to grant or refuse access; it is likely that this will depend on the contractual relationship between the parent and the school.

Some types of personal data are exempt from the right of a SAR and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have. There are also some restrictions on disclosing information in response to a SAR, for example, where this would involve disclosing information about another individual.

If the individual requests for non-personal information, then this cannot be treated as a SAR. (ICO, p.14) In this case, the governing body or LA can treat this as two requests:

- The request for personal data under the Data Protection Act 1998

- Any remaining or non-personal information under the Freedom of Information Act 2000

## DEFINITION OF EDUCATIONAL RECORD

Schools dealing with an SAR will most commonly release information held on a student's educational record. Whilst personal information, held and processed by the school, about current and past students can be legally disclosed to a requester, some information is exempt from being released. (ICO, p.48)

Information kept by a teacher solely for their own use is not classed as part of an educational record. Similarly, data about the pupil provided by a parent of another child cannot be disclosed.

## CONSIDERING THE REQUEST

It is necessary for the Trust to weigh the referee's interest in having their information treated confidentially against the requester's interest in seeing the information. (ICO, 2014) The school must consider the following:

- Any reasons the referee may give for withholding consent
- Any clearly stated assurance of confidentiality given to the referee
- The impact of the information on the requester
- Any risk that disclosure of the information may pose to the referee
- Whether it has been recorded solely for the teacher's purpose (DfE, p.72)

## THIRD PARTY INVOLVEMENT

In terms of providing information that relates to a third party, the Data Protection Act 1998 says you do not have to comply with a request if it involves disclosing information about another individual who can be easily identified by the information. (DfE, 1998)

The Trust must consider whether it is appropriate to disclose information involving another individual. This decision will involve balancing the requester's right of access against the third party's rights in respect of their own personal data. (ICO, p.51)

Third party data can be disclosed in the following circumstances:

- The other individual has consented
- It is reasonable to comply with the request without third party consent
- The information has only been supplied by the third party
- The information does not directly involve the third party

## REFUSING A REQUEST

Where an exemption applies to the facts of a particular request, you may refuse to provide all or some of the information requested, depending on the circumstances. (ICO, p.112) An SAR can be entirely refused under the following circumstances:

- It would cost too much or take too much staff time to deal with the request

- The request is vexatious
- The request repeats a previous request from the same person
- The information is already reasonably accessible to the parent by other means
- The information is likely to cause serious harm to the physical or mental health of the pupil or another individual
- The information is from or including a third party (e.g. child or different parent)
- The information has been recorded solely for the teacher's purpose