Birdsedge First School

Data protection and use of information policy – Key responsibilities

Introduction

We all have responsibilities for using protecting personal data and using information responsibly. To ensure that this happens on a consistent basis throughout our organisation this will be made clear to all that are part of our data ecosystem, and specific responsibilities will be given to ensure there is clarity around accountability and responsibility for particular areas of implementing the policy.

The responsibilities of the various parties affected by this policy are as follows:

A. Board of Trustees

The Board of Trustees of The Mast AcademyTrust is ultimately responsible for ensuring that the Data protection and use of information policy in place complies with the General Data Protection Regulations and satisfies other guidance relating to the use of information in schools.

They will monitor the policy and ensure recommendations and reports submitted to them by the ICO or Data Protection Officer are given due consideration and action taken as necessary.

The Board of Trustees will receive the data audit, data impact assessment and information regarding any data breaches and information requests for the school during the course of the year and ensure that action is being taken to maintain high standards of data management.

The Board of Trustees will review the data protection and use of information policy and its schedules on a periodic basis to ensure that the policy remains coherent and up to date.

The Board of Trustees will also be asked to ensure the oversight of the implementation of any actions as agreed at meetings from time to time.

The Board of Trustees will be responsible for appointing the Data Protection Officer on an annual basis.

B. Local Governing Body

The Local Governing Body has a responsibility for ensuring that the principles of data protection and use of information are applied at the school.

This will include monitoring the policy on a periodic basis to ensure that standards are in place relating to the protection of personal data and use of information in the school.

The Local Governing Body will be responsible for liaising with the Data Protection Officer and Headteacher in the case of any personal data breach and requests for information and will report this to the Trust if it is decided serious enough to be reported to the Information Commissioners Office.

The Local Governing Body has the authority to scrutinise the arrangements for data protection at the school and will receive on an annual basis a report from the Data Protection Officer with regard to the suitability of internal controls at the school.

C. Headteachers

Headteachers are responsible for reporting to the Local Governing Body with respect to the operation of the data protection and use of information at school policy at school level and updating the LGB on any actions as requested.

Headteachers are also responsible (and may delegate this responsibility to suitably qualified staff) for ensuring that only necessary access to data is given to all members of the school's community (e.g. pupils / staff / governors / visitors / contractors).

Headteachers are responsible for ensuring all users of data in the school (including visitors) are given appropriate training and/or information to ensure compliance with regulations and the highest standards of information security.

The Headteacher will be responsible for organising investigations into inappropriate use of information and ensuring actions are taken to minimise the risk of re-occurrence.

D. Data Protection Officer

The Data Protection Officer has specific responsibilities laid out in the General Data Protection Regulations. The principles of these are laid out below:

To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.

To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

In carrying out these responsibilities, the Data Protection Officer will report to the Board of Trustees and submit reports and recommendations regarding the operation of the policy. The Board of Trustees will ensure that the Data Protection Officer is protected from any disciplinary action with regards to carrying out their duty with regards to the GDPR.

The Data Protection Officer will be appointed on an annual basis and will work under the direction of the Governing body, having access to inform this decision making body directly.

E. Third- party data processors

Where external companies are used to process personal data on behalf of the school, accountability for the security and appropriate use of that data remains with the school and ultimately the LGB.

Where a third-party data processor is used:

- a data processor must be chosen providing sufficient guarantees and evidence about its ability to protect the personal data of the data controller's data subject.
- reasonable steps must be taken that such security measures are in place, including written or contractual evidence that data security measures are in place with regards to relevant data.
- Further assurances regarding data processed outside of the United Kingdom must be sought in order to ensure that appropriate security is in place for the processing of this data.

F. Pupils and other children accessing data

Pupils will be given clear guidance on the acceptable use of information within their school life. It is their responsibility to adhere to these guidelines and ensure that they follow the school's guidance in this area.

They are expected to adhere to all of this guidance and any breaches will be investigated and further action may be taken.

Further details of what their responsibilities with regard to this can be found in the Acceptable use of IT schedule.

G. Staff

Staff and other users may be given access to data and use this in the course of doing their work or employment. It is their responsibility to ensure that data that they have access to will be treated within the guidelines outlined. Each of these individuals will be given training on the use of data and protecting the rights of data subjects. Failure to comply may result in disciplinary action against the individual.

H. Other users of information

Other users of information in the school must be given guidance on what information they are able to access. This will be designed to absolutely minimise access to personal data and will be within a clearly defined lawful reason, supported by a data sharing agreement where appropriate. When being given access to this information the school will monitor that this information is the only information being accessed. It is the responsibility of these users to access only the information agreed and misuse of information will lead to corrective action up to and including legal action and remedies.