Discovery Schools Academy Trust

DSAT Data Protection Policy 2016

The Executive Board of Directors of Discovery Schools Academies Trust Ltd adopted this policy

To be reviewed Annually

Scope

This policy applies to all Discovery Schools Academies Trust schools, *(and within this policy will be referenced as DSAT or Company)*, and is to be read in conjunction with the Social Media, Remote Working from Home and ICT Acceptable Use Policies.

Purpose

Discovery Schools Academies Trust Ltd is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents, governors and directors.

Introduction

1. Discovery Schools Academies Trust Ltd needs to keep certain information about employees, pupils and other users to allow the Company, for example, to monitor performance, achievement, and health and safety.
2. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Company and all employees of the Company must comply with the Data Protection Principles which are set out in the Data Protection Act 1998.
3. In summary these principles state that personal data shall:

   i. Be obtained and processed fairly and lawfully.
   ii. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
   iii. Be adequate, relevant and not excessive in relation to their purpose.
   iv. Be accurate and kept up-to-date.
   v. Not be kept for longer than is necessary for that purpose.
   vi. Be processed in accordance with the data subject's rights.
   vii. Be kept safe from unauthorised access, accidental loss or destruction.

4. All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Company has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Company from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

1. The Company, as a body, is the Data Controller under the 1998 Act, and the Directors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.
2. The Company has identified its Designated Data Controllers as:

i. CEO
ii. Director of Operation
iii. Head teachers of individual schools
iv. Business or Office Managers of individual schools.

3. Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Head Teacher, in the first instance. Where issues cannot be resolved with the Head Teacher the matter should be referred to the System Leader and then to the CEO.

Responsibilities of Staff

All staff are responsible for:

1. Checking that any information that they provide to the Company in connection with their employment is accurate and up to date.
2. Informing the Company via their workplace school, of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The Company cannot be held responsible for any errors unless the staff member has informed the Company via their workplace school of such changes.
3. Handling all personal data (eg – pupil attainment data) with reference to this policy.

Data Security

All staff are responsible for ensuring that:

1. Any personal data that they hold is kept securely and they uphold the principles of a 'Clear Desk' policy – which involves the removal of physical records that contain sensitive or personal information to a cupboard or drawer (lockable where appropriate).
2. Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
3. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.
4. Personal information should:
   - Be kept in a filing cabinet, drawer, or safe in a secure office, or;
   - If it is computerised, be encrypted both on a local hard drive and on a network drive that is regularly backed up; and
   - If a copy is kept on a USB memory key or other removable storage media, that media must itself be encrypted and/or kept in a filing cabinet, drawer, or safe.
5. Any System backups should be encrypted.

Rights to Access Information

All staff, parents and other users are entitled to:

1. Know what information the Company holds and processes about them or their child and why.
2. Know how to gain access to it.
3. Know how to keep it up to date.
4. Know what the Company is doing to comply with its obligations under the 1998 Act.

The Company will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them, this is referred to as the Privacy Notice. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Head teacher in the first instance. The Head teacher will ask to see evidence of your identity, such as your passport or driving license, before disclosure of information.

The Head teacher may make a charge on each occasion that access is requested in order to meet the costs of providing the details of the information held.

The Company aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Retention of Data

The Company has a duty to retain some staff and pupil personal data for a period of time following their departure from the Company, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time and stored in hard copy or electronically.

Data will only be kept for the agreed period of time and for the purpose for which it was intended and will be disposed of in accordance with the Companies records management guidelines. Please refer to:
http://www.irms.org.uk/images/resources/2016_IRMS_Toolkit%20for%20Schools_v5_Master.pdf
Appendix 1 – Retention of Data
Appendix 2 – DSAT Remote Working from Home Policy
Appendix 3 – DSAT Bringing your own Devices to Work (TBC)

Monitoring and Evaluation

This is ongoing; where any clarifications or actions are needed the Policy will be amended at its next review. Review frequency: Every 2 years