Codsall
Multi-Academy Trust

Data Protection Policy 2016

St Nicholas CE (VC)
First School
learning and believing, growing and achieving

Codsall
Middle School

CMAT Data Protection Policy

Introduction

Data Protection legislation imposes strict obligations on Codsall Multi-Academy Trust (CMAT) and its employees that are designed to protect the rights of individuals with regard to the safeguarding of their personal data.

The Chief Executive Officer of the MAT has been appointed as the Data Protection Officer and has direct responsibility for ensuring that all these obligations have been fulfilled. A breach of this policy represents serious misconduct and may be the subject of disciplinary action, up to and including dismissal.

Scope

This policy applies to all directors, governors, staff and pupils of CMAT. It also applies to parents and carers of pupils at schools within the MAT, who formally confirm that they will abide by our policies when their children join our schools. Each school within the MAT must ensure that the contents of this policy are communicated to all staff. This communication must be evidenced in writing and refreshed on an annual basis. All parents must formally accept this policy when their children join a MAT school and this acceptance must be evidenced in writing through the Home-School Agreement. Each school within the MAT must publish this policy on its website.

Definitions

Authorised Locations - A place approved by the DPO for the storage of Personal Data.

CEO - Chief Executive Officer.

Data Access Request - A formal request from a Data Subject to access Personal Data. These do not need to be in writing and there is a limited time period under law to respond to them.

Data Subject - The individual to whom the Personal Data relate.

External Data Processors - Third party organisations or individuals that provide the MAT with data processing services. These can include:

- Payroll and management of employees
- Data archiving/destruction
- Website hosting services
- Courier and despatch services
- Confidential waste destruction
- Business or operational administration

- Management Information System (MIS)
- Any outsourcing activity

Personal Data

Any data that relate to and can, whether on its own or in conjunction with other information, specifically identify an individual living person. Personal data includes, for example, names and addresses, e-mail addresses, recruitment details as well as personal, health or performance records. They also include opinions about individuals as well as facts and also apply to corporate contacts. Personal data includes data held electronically on a computer or network, data held in hard copy paper format and web based data.

Processing: This is a wide-ranging term that, in practice, covers any use of Personal Data including:

- Obtaining, recording, holding, and carrying out any operation(s) on the Personal Data
- Organisation or alteration of the Personal Data
- Retrieval, disclosure or use of the Personal Data

All such data processing activities will constitute Processing within the meaning of data protection laws.

Sensitive Personal Data Any information about an individual's physical or mental health, racial or ethnic origin, sexual life, politics, religion, trade union membership, or any information about alleged or committed criminal offences.

Policy

1. The CEO is responsible for the implementation and operation of this policy and performs the role of Data Protection Officer (DPO).

2. Personal data must not be held longer than is necessary.

3. Personal data should be held according to the retention periods agreed for each business area. If there is no clear agreement for the area or the type of data, then the personal data should not be kept for any longer than is reasonably necessary for the purpose for which it was collected.

4. Personal data must only be stored at authorised locations, as determined by the CEO.

5. Personal data must be kept accurate and up to date, and must be adequate, relevant and not excessive.

6. Reasonable steps must be taken to ensure the accuracy and quality of personal data, and to prevent it from becoming out of date. Periodic reviews of the information held should be completed to ensure on-going accuracy. If data are found to be out of date or inaccurate, they must be corrected as soon as is reasonably possible.

7. All processing of personal data must be adequate, relevant and not excessive for the specific purposes for which the data was obtained. The most appropriate time for informing the data subject with notice of the purposes of collection is at the time the personal data are collected.

8. Any processing of personal data must be necessary to achieve the purpose for which it was collected and the data subject must not be misled or deceived with regards to the purposes or extent of the processing of their personal data.

9. Directors, governors and staff must not process or store sensitive personal data unless this is necessary and then only if the individual has explicitly consented. A record of that consent must be retained and be available for inspection for at least two years after the sensitive personal data are no longer being processed or stored.

10. Personal data must be stored and managed securely and all staff must take precautions against physical loss or damage. They must also ensure that both access to and disclosure of personal data is restricted as appropriate. In particular:

a. Personal data must not be disclosed, either orally or in writing or otherwise, to an unauthorised third party without a clear "need to know" reason being identified prior to disclosure and in accordance with the notice provided to the data subject.

b. When physical personal data are left unattended, they must be secured – for example within locked office furniture. Personal data in electronic form must be inaccessible when left unattended.

c. Files containing personal data must not be left in open view.

d. Personal data stored on laptop computers and mobile phones are subject to the provisions of this policy.

11. A data subject must be given notice of the purposes for which their personal data is being processed and personal data must only be processed for these purposes.

12. Data subjects have the right, subject to certain exceptions and procedural requirements, to access personal data that is being processed about them, through the means of a Data Access Request. The MAT is required by law to respond to such a request within 40 days, either by providing the data or explaining why it is subject to a relevant exemption. Any director, governor or member of staff receiving a Data Access Request must immediately forward it to the DPO. Under no circumstances should anyone respond directly to a Data Access Request unless they are specifically requested to do so by the DPO.

13. A Data Access Request may be received in an email or letter. The DPO should be notified of the request and of your response.

14. Data subjects have the right to require the MAT to correct any inaccurate data held about them. The MAT is legally required to respond to such a Request within 21 days of receiving it. Any requests for inaccuracies to be corrected must be immediately forwarded to the DPO. The MAT has a legal obligation to comply with such requests provided that the

Data Subject has been satisfactorily identified. The person receiving the request should take reasonable steps to identify the data subject before forwarding the request to the DPO.

15. Data subjects' rights must be observed and directors, governors and staff must take all reasonable steps to ensure that they are aware of and respect these rights. These rights include:

a. Right to prevent damage – an individual can take steps to prevent the processing of data that may cause substantial damage or distress.

b. Right to prevent automated decisions – individuals can request that decisions made about them by automatic means be retaken manually.

c. Right to request an assessment – individuals can ask the relevant data protection authority to assess whether or not, in a particular instance, data are being processed in accordance with data protection laws within the MAT.

16. No employee is authorised to deal with an external data processor without the approval of the DPO who must ensure that they adopt appropriate technical and organisational security measures to safeguard personal data and that these measures are managed appropriately.

17. Accessing, deleting or otherwise using any information that is not part of a director's, governor's, or employee's duties or without prior authority is a serious disciplinary offence and may be subject to sanctions.

Disputes

18. Anyone who has a concern or complaint regarding the application of this policy should contact the DPO. In the event that the DPO cannot address the concern, the concern or complaint should be referred to the Chairman of the MAT. This does not impact or override any legal remedies available.

Review

19. The policy owner must keep up to date with relevant legislation and government guidance and update this policy whenever necessary. The board of the MAT must approve the revised version.

20. The policy owner must review the policy at the end of July each year and either submit a revised policy for board approval or confirm in writing to the CEO that the current version of this policy is still fit for purpose.

21. The CEO must submit a list of all confirmed policies to the board at the first meeting of each new academic year.

22. The MAT board must formally review and re-approve this policy every five years.

Date of Policy Approval: January 2017

Date of Policy Review: January 2022

Signed

Mr K McElduff Chairman of Trustees

Codsall Multi Academy Trust