APPROPRIATE POLICY

Approved by the Learning and Standards Committee

08.06.22

DUE FOR RENEWAL: FEBRUARY 2024

FEBRUARY 2022

CHANGES

Feb 2022	Policy implemented

CONTENTS

1. Introduction 4
2. What is data processing? 4
3. What is special category data? 4
4. What is criminal conviction data? 4
5. Condition for processing 4
6. Principles 5
7. Retention and erasure policies 6
8. Appropriate policy review date 6

1. INTRODUCTION

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Discovery Multi Academy Trust will process special category data to carry out its statutory functions or legal obligations. In accordance with Schedule 1 Part 4 of the Data Protection Act, this document explains how the Trust complies when processing Special Category Data and Criminal Conviction data.

2. WHAT IS DATA PROCESSING?

The GDPR defines this as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. WHAT IS SPECIAL CATEGORY DATA?

The GDPR defines this as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. WHAT IS CRIMINAL CONVICTION DATA?

The GDPR defines this as personal data relating to criminal convictions and offences or related security measures. The Data Protection Act adds that this also includes allegations of the commission of offences, criminal proceedings and sentencing.

5. CONDITION FOR PROCESSING

Discovery Multi Academy Trust has identified the following conditions for processing this special category data:

- Sch. 1, Part 1, para. 1: Employment, social security, and social protection.
- Sch. 1, Part 2, para. 6: Statutory etc. and government purposes.
- Sch.1, Part 2, para. 7: Administration of justice.
- Sch. 1, Part 2, para. 8: Equality of opportunity or treatment.
- Sch. 1, Part 2, para. 9: Racial and ethnic diversity at senior levels of organisations
- Sch. 1, Part 2, para. 10: Preventing or detecting unlawful acts.
- Sch. 1, Part 2, para. 11: Protecting the public against dishonesty
- Sch. 1, Part 2, para. 12: Regulatory requirements relating to unlawful acts and dishonesty etc.
- Sch. 1, Part 2, para. 14: Preventing fraud.
- Sch. 1, Part 2, para. 18: Safeguarding children and of individuals at risk.
- Sch. 1, Part 2, para.19: Safeguarding of economic well-being of certain individuals
- Sch. 1, Part 2, para. 21: Occupational pensions
- Sch. 1, Part 2, para. 24: Disclosure to elected representatives

6. PRINCIPLES

Procedures are in place for securing compliance with the Data Protection Principles in relation to the processing of Special Category and Criminal Conviction Data. They are outlined below.

Accountability principle
• The trust take responsibility for complying with the UK GDPR at the highest management level and throughout the organisation. The Chief Executive Officer has ultimate responsibility. • All staff receive regular training and are aware of their own responsibilities. The Head of School has accountability at school level. • The trust maintains a Data Asset Register and Retention Schedule to record our processing activities. • The trust has an appropriate data protection policy and other associate policies and procedures in place, such as breach management and data subjects' rights, which are reviewed regularly. • The trust carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests. The trust take additional care with the processing of children's personal/special category data as they are less able to understand their rights. • The trust employ the services of a Data Protection Officer from the Local Authority. • The trust implement appropriate security measures for all types of processing of personal and special category data.
Principle (a): lawfulness, fairness and transparency
• We ensure that we have identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data. • Privacy notices are available on the school website and we ensure that data subjects receive privacy information so that processing is transparent. • The trust are very open and honest with our data subjects or parents where the collection of SC/CO data is required. We are careful not to deceive or mislead people about its use. • We will not do anything unlawful with the information. • The trust have considered how the processing may affect the individuals concerned and ensure that we only process information fairly.
Principle (b): purpose limitation
• The purposes for processing the SC/CO data have been clearly identified and are documented in our data asset register and our privacy notices. • If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), the trust will check that this is compatible with our original purpose or get specific consent for the new purpose. • If we do use personal data for a new purpose, that is compatible, we will inform the data subject first. • We regularly review our processing and update our documentation if necessary.
Principle (c): data minimisation

- The trust have reviewed the special category data that they collect and are satisfied that we are only collecting SC/CO personal data that we actually need for our specified purposes.
- The SC/CO data that we collect is sufficient to properly fulfil those purposes.
- We do carefully review this particular SC/CO data, and will delete, anonymise or redact anything we don't need.

Principle (d): accuracy

- The trust record the source of the SC/CO data we collect.
- The trust will ensure that the personal data we hold is accurate and kept up to date as necessary. Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that it is erased or rectified without delay. If we decide not to either erase or rectify it, we will document our decision.
- The trust have policies in place that will ensure the regular review of the accuracy of certain special category data, such as medication or individual health care plans, risk assessments, EHCP's etc.
- The trust have a Subject Rights Request Policy which outlines how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification?

Principle (e): storage limitation

- The trust will only keep the SC/CO data for as long as we need it or to comply with any statutory retention requirements. We can justify this amount of time.
- We have a retention schedule that clearly defines how long we can retain SC/CO data, once it is no longer in use and what happens to that data at the end of the retention period, e.g. destruction/anonymisation.
- These periods are determined variously by the needs of the trust and relevant legislative and regulatory requirements. The trust use education best practice guidelines as a benchmark.
- The School's data asset register and retention schedule clearly identifies any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes, if applicable.
- We have a Data Retention and Safe Destruction Policy.
- The School regularly reviews the data in line with the retention schedules and destroys or renders permanently anonymous personal data that we no longer need.

Principle (f): integrity and confidentiality (security)

- Potential risks have been identified with appropriate mitigation. Third party suppliers or data processors used to process SC/CO data have had DPIA's and/or other appropriate data protection and security checks completed.
- Hard copy SC/CO data is stored in locked filing systems.
- All personal and SC/CO, whether hard copy, electronic or on-line have restricted access to only those that require access for the role they perform.
- The trust has an information security policy which covers this SC/CO data and we make sure the policy is implemented and reviewed regularly.
- The trust has a process to back-up data and we can restore access to personal data in the event of any incidents.
- We put necessary technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing.
- The trust takes all necessary steps to ensure the confidentiality, integrity and availability of the data we are processing.
- The trust carries out regular testing and reviews of our measures to ensure they remain effective.

7. RETENTION AND ERASURE POLICIES

The trust has a data asset register and retention schedule. This sets out the type of data being processed, including whether this is/includes special category data and how long we keep this information for. This is a link to the register GDPR - Home (sharepoint.com)

Data subjects receive full privacy information about how their data will be handled, and this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

8. APPROPRIATE POLICY REVIEW DATE

The trust will review this policy every two years.