COMDA-08-APPROPRIATE POLICY DOCUMENT

1 INTRODUCTION

1.1 This is a document required by the Information Commissioners Officer (ICO).

1.2 It must be called the Appropriate Policy Document.

1.3 It ensures that the Trust is allowed to process SC (Special Category) and Criminal Offence (CO) data.

1.4 Having this in place ensures that the Trust is compliant with Schedule 1, paragraphs 1(1)(b) and 5, and Schedule 1, Part 2 of the DPA 2018.

1.5 This policy covers all of the processing of SC and CO data by the Trust.

1.6 The policy must be regularly reviewed and must be retained until 6 months after the relevant processing ceases.

1.7 If the ICO requests sight of this document, it must be provided free of charge.

2 ROLE OF TRUST BOARD AND COMMITTEES

2.1 Outline of respective responsibilities per Scheme of Delegation.

3 ROLE OF PRINCIPAL AND SENIOR LEADERSHIP TEAM

3.1 Outline of respective responsibilities per Scheme of Delegation and other related policies.

4 DESCRIPTION OF DATA PROCESSED

4.1 Personal data which could reveal racial or ethnic origin.

4.2 Personal data which could reveal religious or philosophical beliefs.

4.3 Personal data which could reveal trade union membership.

4.4 Genetic data.

4.5 Biometric data.

4.6 Data relating to the health of a person.

4.7 Data relating to a person's sex life or sexual orientation.

5 SCHEDULE 1 CONDITION FOR PROCESSING (LINK)

5.1 Article 9:

5.1.1 (b) Employment, social security, and social protection

5.1.2 (h) Health or Social Care

5.2 Schedule 1, Part 1:

5.2.1 1(1)(a) The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law or the controller or the data subject in connection with employment, social security, or social protection.

5.2.2 2(1)(2)(f) The management of health care systems or services or social care systems or services.

5.3 Schedule 1, Part 2

5.3.1 8(1)(b) Is necessary for the purposes of identifying or keeping under review the existence or absence of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained.

5.3.2 16(1)(c) providing support to individuals with a particular disability or medical condition.

5.3.3 17(1)(a) is necessary for the provision of confidential counselling, advice, or support.

5.3.4 18(1)(a) protecting an individual from neglect or physical, mental, or emotional harm or protecting the physical, mental, or emotional well-being of an individual.

5.3.5 18(1)(b) when the individual is aged under 18 or aged over 18 and at risk.

5.4 Privacy Document for The Trust

6 ACCOUNTABILITY PRINCIPLE

6.1 The Trust is developing appropriate documentation of its processing activities.

6.2 The Trust has an appropriate data protection policy (in U:\Staff Information\Policies).

6.3 The Trust completes data protection impact assessments (DPIAs) for all new uses of personal data, and is producing them retrospectively, for those uses of personal data which were established earlier.

7 PRINCIPLE (A): LAWFULNESS, FAIRNESS AND TRANSPARENCY

7.1 The lawful bases for processing and further Schedule 1 conditions for processing SC/CO data are stated in point 5.

7.2 Appropriate privacy information for all information, including SC and CO, is made available via a subject access request (SAR).

7.3 The Trust is open and honest when it collects the SC/CO data; it ensures that it does not deceive or mislead people about the use of this data.

8 PRINCIPLE (B): PURPOSE LIMITATION

8.1 The Trust has clearly identified its purpose or purposes for processing.

8.2 The Trust has documented those purposes.

8.3 The Trust has included details of its purposes in its privacy information for individuals.

8.4 The Trust regularly review its processing and, where necessary, update its documentation and its privacy information for individuals.

8.5 If The Trust has plans to use personal data for a new purpose other than a legal obligation or function set out in law, it will check that this is compatible with its original purpose or get specific consent for the new purpose.

9 PRINCIPLE (C): DATA MINIMISATION

9.1 The Trust only collects personal data it actually needs, for its specified purposes.

9.2 The Trust has sufficient personal data to properly fulfil those purposes.

9.3 The Trust periodically reviews the data it holds and delete anything it doesn't need.

10 PRINCIPLE (D): ACCURACY

10.1 The Trust ensures the accuracy of any personal data it creates.

10.2 The Trust has appropriate processes in place to check the accuracy of the data it collects, and it records the source of that data.

10.3 The Trust has a process in place to identify when it needs to keep the data updated to properly fulfil its purpose, and this is updated as necessary.

10.4 If the Trust needs to keep a record of a mistake, it will clearly identify it as a mistake.

10.5 The Trust records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.

10.6 The Trust complies with the individual's right to rectification and carefully considers any challenges to the accuracy of the personal data.

10.7 As a matter of good practice, the Trust keeps a note of any challenges to the accuracy of the personal data.

11 PRINCIPLE (E): STORAGE

11.1 The Trust knows what personal data it holds and why it needs it.

11.2 The Trust carefully considers and can justify how long it keeps personal data.

11.3 The Trust has a policy with standard retention periods where possible, in line with documentation obligations. (This retention policy is in U:\Staff Information\Policies).

11.4 The Trust regularly reviews its information and erases or anonymises personal data when it no longer needs it.

11.5 The Trust has appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.

11.6 The Trust clearly identifies any personal data that it needs to keep for public interest archiving, scientific or historical research, or statistical purposes.

12 PRINCIPLE (F): INTEGRITY AND CONFIDENTIALITY (SECURITY)

12.1 The Trust undertakes an analysis of the risks presented by its processing and uses this to assess the appropriate level of security it needs to put in place.

12.2 When deciding what measures to implement, The Trust takes account of the state of the art and costs of implementation.

12.3 The Trust has an information security policy (or equivalent) and takes steps to make sure the policy is implemented.

12.4 Where necessary, The Trust has additional policies and ensures that controls are in place to enforce them.

12.5 The Trust makes sure that it regularly reviews its information security policies and measures and, where necessary, improves them.

12.6 The Trust has assessed what it needs to do by considering the security outcomes it wants to achieve, such as:

12.6.1 managing security risk

12.6.2 protecting personal data against cyber-attack

12.6.3 detecting security events

12.6.4 minimising the impact

12.7 The Trust has put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.

12.8 The Trust understands that it may also need to put other technical measures in place depending on its circumstances and the type of personal data it processes.

12.9 The Trust uses encryption and/or pseudonymisation where it is appropriate to do so.

12.10 The Trust understands the requirements of confidentiality, integrity, and availability for the personal data it processes.

12.11 The Trust makes sure that it can restore access to personal data in the event of any incidents and has an established appropriate backup process.

12.12 Where appropriate, The Trust implements measures that adhere to an approved code of conduct or certification mechanism.

12.13 The Trust ensures that any data processor it uses also implements appropriate technical and organisational measures (this is through the process of writing/reviewing a DPIA).

13 RETENTION AND ERASURE POLICIES

13.1 The Trust has a policy with standard retention periods where possible, in line with documentation obligations. (This retention policy is in U:\Staff Information\Policies)

14 POLICY AUTHOR

14.1 The author of this policy is the Data Protection Officer. They should be contacted for any points of clarification or suggested future amendments.

15 VERSION CONTROL

Policy Number	COMDA-08-
Policy Name	Appropriate Policy Document
Version Number	02
Publication Method	External A copy must be made available in U:\Staff Information\Policies\COMmunications and DAta Policies
Approved by	Full Trust Board
Date of Approval	October 2023
Key changes since previous version	Checked against ICO template. No changes required
Next Review Date	September 2024