COMDA-03-DATA PROTECTION

1 INTRODUCTION

1.1 This policy sets out how all staff and the Trust Board will ensure that personal and sensitive personal data is dealt with correctly and securely and in accordance with the General Data Protection Regulations (GDPR), and other related legislation.

1.2 The Trust processes personal data relating to students, staff, governors, visitors and parents and is therefore a data controller.

1.3 In accordance with the regulations, the Trust is registered as a Data Controller with the Information Commissioner's Office (ICO). This is renewed annually.

1.4 The register is available to view here: http://www.ico.org.uk/what_we_cover/register_of_data_controllers

1.4.1 The Data Protection Act 2018 (DPA2018), and the General Data Protection Regulations (GDPR) establishes a framework of rights and duties which are designed to protect and enforce the privacy of personal data whilst also allowing for the lawful and appropriate use, sharing or transfer of this type of data.

1.5 The Regulations are underpinned by a set of six principles. The Trust is committed to following these principles as set out in this policy. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

2 ROLE OF TRUST BOARD AND COMMITTEES

2.1 The Trust Board has overall responsibility for ensuring compliance with all relevant data protection obligations.

3 ROLE OF PRINCIPAL AND SENIOR LEADERSHIP TEAM

3.1 The Principal acts as the representative of the Data Controller on a day-to-day basis.

3.2 The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. They will report directly to the Principal and Trust Board on any data protection issues or recommendations. The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

3.3 The DPO role is shared with SMBC's Information Governance Team.

4 DEFINITIONS

4.1 **Personal Data –** Any information relating to an identified, or identifiable, living individual. This includes but is not limited to:

- Names;
- Email addresses;
- ID numbers;
- Images;
- It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

4.2 **Special Categories of Personal Data –** previously referred to as 'Sensitive Personal Data'; this includes information about an individual's racial or ethnic origin, political opinions, religious beliefs and trade union memberships. It also includes an individual's genetic or biometric data (including fingerprints) and any data relating to an individual's physical, mental or sexual health.

4.3 **Processing –** Any automated or manual act involving personal data such as collecting, storing, altering, using, sharing/transporting and destroying.

4.4 **Data Subject –** The individual whose personal data is being held or processed.

4.5 **Data Controller –** A person or organisation that determines the purposes and means of processing personal data.

4.6 **Data Processor –** A person or body that processes data on behalf of the data controller.

4.7 **Information Commissioner's Office** (ICO) – This is the statutory regulator for data protection and information processing.

4.8 **Data Protection Officer** (DPO) – the person at the Trust who manages and oversees data protection.

4.9 **Regulations/GDPR** – The General Data Protection Regulations which became law with the Data Protection Act in May 2018.

4.10 **On Site** – the Gipsy Lane campus, car parks, yards, fields and buildings. This specifically excludes Holly Lane.

4.11 **Off Site** - everywhere else.

5 STAFF

5.1 This policy applies to all staff employed by the Trust, and to external organisations or individuals working on our behalf (referred to as "Staff" for the rest of this policy). This includes supply staff and volunteers.

5.2 Those who do not comply with this policy will face disciplinary action.

5.3 All Staff are required to comply with this policy under the following circumstances:

- Collecting, storing and processing any person's personal data;
- Informing the Trust of any changes to their personal data, such as a change of address;
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
    - If there has been a data breach or they have any concerns that there may have been a data breach;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they need help with any contracts or sharing personal data with third parties.

6 PRINCIPLES OF THE DATA PROTECTION ACT 2018

6.1 Processing data fairly, lawfully and transparently

6.1.1 The Trust will inform students, staff, parents/carers and any other data subjects why they need their personal data, how it will be used and with whom it may be shared. This will be done via Privacy Notice documents issued with the appropriate data collection form and also via the website where this is necessary.

6.1.2 The Trust will process personal data with regard to the conditions laid out in the GDPR and where appropriate consent will be sought.

6.1.3 The Trust will only process personal data lawfully.

6.2 Processing data for specific, explicit purposes

6.2.1 Personal data held will only be used for statutory purposes as outlined in the Trust's Privacy Notice unless explicit and affirmative consent has been granted.

6.2.2 Data will only be shared with external parties where a statutory basis exists to do so or we have acquired consent.

6.2.3 Where data is shared outside of the European Economic Area (EEA), including with cloud providers, checks will be made to ensure an adequate level of protection for that information and consent will be sought from those affected where required.

6.3 Processing data which is adequate, relevant and limited to only what is necessary

6.3.1 The Trust will endeavour to collect enough personal data that is sufficient for the purpose and will not ask for more information than is necessary.

6.3.2 The Trust will regularly review data collection forms and will check personal data already held for missing, irrelevant or seemingly excessive information

6.4 Ensuring data is accurate and, where necessary, kept up to date

6.4.1 Data held by the Trust will be as accurate and up to date as is reasonably possible and steps will be taken to regularly check the accuracy of personal data held; an example is the annual data form issued to all parents to check all details are up-to-date.

6.4.2 If a student, member of staff, a parent or any other data subject informs the Trust of a change of circumstances or an error the relevant personal data will be updated as soon as is practicable.

6.5 Ensuring data is kept only for as long as it is required

6.5.1 The Trust will not keep personal data for longer than is necessary for the stated purpose(s). In order to ensure this, all information held and/or created by the Trust or held on its behalf will be retained according to timescales set out in the Trust's Data Retention Schedule.

6.5.2 The Trust will ensure that all personal data deleted or physically destroyed is done in a secure and confidential way.

6.6 Ensuring that the data is handled in such a way that ensures appropriate security, including data protection against unlawful or unauthorised processing, access, loss, destruction or damage

6.6.1 To prevent unauthorised/unlawful processing and accidental loss, destruction of, or damage to personal data the Trust will ensure appropriate security measures are in place to safeguard all personal data whether held in paper files, on a computer system, laptop or on portable media storage devices e.g. USB Memory Sticks.

6.6.2 Paper records and portable media storage devices must be kept in a locked room, cupboard or drawer when not in use and only accessed by those authorised to see the information held on them. Portable media storage drives must have added encryption software as standard.

6.6.3 Personal data held electronically is kept securely, is protected by passwords, and is only accessed only by those authorised to see the information held.

6.6.4 The Trust will avoid storing personal information on the hard drive of PCs or portable equipment and media, including, but not limited to, laptops, tablets, tablet PCs, netbooks, memory sticks, external hard drives, CDs and DVDs, but where this is necessary the relevant equipment or portable media will always be encrypted. If it is necessary to take any of these assets outside of the on-site buildings they will be protected in transit using the school-provided bags, they must not be left unattended and they must be stored securely.

6.6.5 Particular care must be taken when sending personal data via emails, faxes and letters, etc. to use secure methods and only to confirmed addresses/numbers. School email is not secure. Data sent to external organisations via email must be encrypted and the password sent separately.

6.6.6 All breaches of this policy will be investigated and may be deemed to be a disciplinary matter.

6.6.7 The Trust will ensure that any contractors who process personal information on the Trust's behalf will do so under clear written instruction and will have adequate safeguards in place to protect the information.

7 RIGHTS OF THE DATA SUBJECT

7.1 The Trust will support the lawful specific rights of any person whose details are held/processed by the Trust, including:

7.1.1 To receive information about how the Trust is collecting their data about how it is used and processed;

7.1.2 A Subject Access Request (to receive a copy of their own personal data) must be passed to the DPO immediately;

7.1.3 Ask the Trust to rectify incorrect data;

7.1.4 Have data erased;

7.1.5 Stop, object or restrict processing of their personal data, in the following circumstances:

- Prevent use of their personal data for direct marketing;
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- Challenge processing which has been justified on the basis of public interest;

7.1.6 Be notified of a data breach (when their personal data has been passed on inappropriately to the wrong person);

7.1.7 Data Portability (allowing data to be transferred for reuse for different services);

7.1.8 Make a complaint to the ICO.

7.2 Individuals should submit any request to exercise these rights to the DPO.

7.3 If staff receive such a request, they must immediately forward it to the DPO.

8 ISSUES SPECIFIC TO THE TRUST

8.1 Consent: When a student is first registered to the Trust, consent for the following will be given by the student (16 and over)/parent:

8.1.1 Photographs/Recordings of students used in Trust publications, including those to be used in the local newspaper and letters;

8.1.2 Photographs/Recordings of students that are used internally by the Trust, for project work;

8.1.3 Photographs/Recordings of students, staff and parents to be used on any web page.
The express consent of the students/parent or staff member must be received due to the potential of the image/recording being viewed worldwide, which may include countries without adequate protection of personal information

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

8.2 CCTV

8.2.1 The Trust uses CCTV to assist with pastoral care and site security.

8.2.2 The CCTV footage will contain personal data.

8.2.3 There must be clear signage in around the Trust's premises explaining that CCTV is in use.

8.2.4 CCTV footage will only be shared with members of Staff who are responsible for pastoral care and site security.

8.2.5 Data is retained in line with the data retention schedule.

8.3 Displays of students' work

8.3.1 Student work that is on display at a public venue (not the Trust premises) the personal data exposed must be kept to a minimum (e.g. First Name, possibly with Year Group).

8.4 Biometric Data

8.4.1 The Trust will notify parents about its use of an automated biometric (fingerprint) recognition system, which is used when staff and students pay for food.

8.4.2 Every person using the system must have consent for this to take place.

8.4.3 An alternative system will be made available for those people who do not want to use the biometric system

8.4.4 Biometric data is a special category of personal data. Use of it is controlled by the Protection of Freedoms Act 2012.

9 COMPLAINTS

9.1 These will be dealt with using the Trust's Complaints Policy.

9.2 Complaints relating to the way that the Trust handles data and information may be referred to the ICO however, they should be referred as follows:

9.2.1 To the Data Protection Officer, for investigation.

9.2.2 If the complaint applies to the DPO then it must be reported to the Principal.

9.2.3 If the complaint applies to the Principal then it must be reported to the Chair of the Trust Board.

10 AUTHOR

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

11 VERSION CONTROL

Policy Number	COMDA-03
Policy Name	Data Protection
Version Number	00
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	8th February 2022
Key changes since previous version	1. Reformatting to current standards 2. Clarification regarding care of devices, sending of data via email, and biometrics 3. Section added on CCTV 4. Addition of definitions 5. Clauses added relating to misconduct
Next review date	February 2023