DATA PROTECTION POLICY

1. Purpose

1.1. This policy sets out how all staff and governors at Heart of England School ('the School') 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.

2. Definitions

2.1. **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.

2.2. **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.

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

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

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

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

3. The Data Controller

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

3.2 In accordance with the regulations, the School is registered as a Data Controller with the Information Commissioner's Office and will renew this annually. The register is available to view here: http://www.ico.org.uk/what_we_cover/register_of_data_controllers

4. Roles and Responsibilities

4.1 This policy applies to all staff employed by the School, and to external organisations or individuals working on our behalf (referred to as "Staff" for the rest of this policy).
Those who do not comply with this policy will face disciplinary action.

4.2 **Governing Body**

The Governing Body of the school have overall responsibility for ensuring compliance with all relevant data protection obligations.

4.3 **Data Protection Officer**

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 Governing Body on any data protection issues or recommendations.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

The current Data Protection Officers for Heart of England School are Joan Fuller and SMBC's Information Governance Team

4.4 **Principal**

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

4.5 **All Staff**

All Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the School 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

5. GDPR and DPA 2018 principles

5.1. In common with its predecessor, The Data Protection Act 1998, 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.

5.2. The Regulations are underpinned by a set of six principles. The School 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

6. Processed Lawfully and Fairly

6.1. The School 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.

6.2. The School will process personal data with regard to the conditions laid out in the Regulations and where appropriate consent will be sought.

6.3. The School will not do anything unlawful with the personal data.

7. Processed for Specified Purpose

7.1. Personal data held will only be used for statutory purposes as outlined in the school Privacy Notices unless explicit and affirmative consent has been granted.

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

8. Adequate, Relevant and Limited

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

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

9. Accuracy

9.1. Data held by the School 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.

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

10. Data Retention

10.1. The School 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 School or held on its behalf will be retained according to timescales set out in the School's Data Retention Schedule.

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

11. Technical and Organisational Security

11.1. To prevent unauthorised/unlawful processing and accidental loss, destruction of, or damage to personal data the School will ensure appropriate security measures are in place to safeguard all personal data whether held in paper files, on a computer system, cloud storage, laptop or on portable media storage devices[1].

11.2. Paper records and portable media storage devices are locked away when not in use and are only accessed by those authorised to see the information held on them. Portable media storage drives have added encryption software as standard.

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

11.4. The School 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 school environment they will be protected in transit, not left unattended and stored securely.

11.5. Particular care will be taken when sending personal data via emails, faxes and letters, etc. to use secure methods where possible and to confirmed addresses/numbers.

11.6. A deliberate breach of this Policy will be treated as disciplinary matter

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

12. Rights of Data Subjects

12.1. The School acknowledges that GDPR gives specific rights[2] to any person whose details are held/processed by the School, including the right to receive a copy of their own personal data.[3]

12.2. A request under this right of access, known as a Subject Access Request should be passed to the DPO immediately and follow the procedures laid out in the separate SAR Procedure.

12.3. In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the school to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress

[1] E.g. USB Memory Sticks, CDs, external hard drives, etc

[2] Right of access to a copy of the personal data held; Right to object to processing that is likely to cause or is causing unwarranted damage or distress; Right to prevent processing for direct marketing; Right to object to decisions being taken by totally automated means; Right to have inaccurate personal information rectified, blocked, erased or destroyed; and a right to claim compensation for damages caused by a breach of the Act.

[3] There are a few exceptions to this rule, but most individuals will be able to have a copy of the information held on them

- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11. School Specific Issues

11.1. Consent

11.1.1. The School will always seek consent/parental consent for the following via an initial consent letter:

- Photographs/Recordings of children used in school publications, including those to be used in the local newspaper and letters.
- Photographs/Recordings of children that are used internally by the school, for school projects.
- Photographs/Recordings of children, staff and parents to be used on any web page. The express consent of the child/parent or staff member must be received due to the potential of the image/recording be viewed worldwide, which may include countries without adequate protection of personal information

11.1.2. 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.

11.2. CCTV

The School utilises CCTV as a means of security. CCTV footage will feature personal data, therefore the School makes sure that students, staff, parents and visitors to School premises are aware that CCTV is in use via clear signage in and around School premises.

11.3. Public Displays

If there is a display of students' work to be shown at a public venue, (other than the school premises), unless they have consent to publish fuller information, the School will only include the minimum of pupil identifiable information, for example "by John, year 1".

11.4. Biometric Data

Biometric data is a special category of personal data and must be processed in accordance with this. In line with the Protection of Freedoms Act 2012 the School will also ensure they have notified parents about their use of an automated biometric recognition system and obtain the required consent from at least one parent of each pupil. The school will always provide alternative means of accessing the relevant services for those students.

12. Complaints

12.1. Complaints will be dealt with in accordance with the School's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator).

13. Contacts including Reporting Breaches

13.1. Any breaches of this policy, including accidental breaches, should be reported immediately to the iDPO using a Breach Record Form unless the breach relates directly to the iDPO, in which case this should be reported to the Principal.

13.2 Where a deliberate breach is suspected this should also be reported to the Principal for further investigation unless the breach relates directly to the Principal, in which case this should be reported to the Chair of Governors.

13.3 Any enquiries regarding this policy or Data Protection in general should be referred to the iDPO in the first instance.

14. Review

14.1. This policy will be reviewed and updated as necessary to reflect best practice or amendments made to GDPR and DPA 2018.