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 Data Protection Act 1998 ('the Act'), and other related legislation.

1.2. This policy should be read in conjunction with the school's Confidentiality Policy.

2. About Data Protection Act

2.1. The Data Protection Act 1998 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.

2.2. The Act applies to anyone who processes personal data. It covers all personal information[1] regardless of its format or the way it is collected, used, recorded, updated, stored and destroyed.

2.3. The Act is underpinned by a set of eight straightforward principles. The School is committed to following these eight principles as set out in this policy.

2.4. Personal data relates to a living individual who can be identified either by that data or along with other information likely to come into a person's possession. This will apply to pupils, staff, parents and others who have contact with the School.

2.5. Personal data also covers facts and opinions about the individual(s) as well as information regarding the intentions of the school towards the individual(s).

3. Processed Fairly and Lawfully

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

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

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

4. Processed for Specified Purpose

4.1. Personal data held for these stated purposes will not be used for any other incompatible purpose without consent

4.2. In accordance with the Act, 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

[1] 'Sensitive' personal data is also covered by the Act

5. Adequate, Relevant and Not Excessive

5.1. 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.
5.2. The School will regularly review data collection forms and will check personal data already held for missing, irrelevant or seemingly excessive information.

6. Accuracy

6.1. 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.
6.2. 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.

7. Data Retention

7.1. 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 Records Management Toolkit for Schools created by the Information and Records Management Society.
7.2. The School will ensure that all personal data deleted or physically destroyed is done in a secure and confidential way.

8. Rights of Data Subjects

8.1. The School acknowledges that the Data Protection Act 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]
8.2. The School will ensure clear procedures are in place to allow for this right of access, known as a Subject Access Request and will supply the information sought within the required 40 calendar days from date of written request.
8.3. Where it is clear a pupil does not understand the nature of subject access request, a written request from parents/carers in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be supplied to the parents/carers.
8.4. The rules of Data Protection apply equally to staff information as they do to pupil data. Staff have a right to view information held by the school about them.
8.5. Any third party data (information about someone other than the requesting individual) found will generally be removed or redacted unless third party permission to disclose is provided or it is reasonable in all circumstances to disclose it.

[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

9. Technical and Organisational Security

9.1. 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, laptop or on portable media storage devices[4].

9.2. 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.

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

9.4. 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.

9.5. 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.

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

9.7. 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.

10. Transfers outside of Europe

10.1. The School is unlikely to transfer any personal information outside of the European Economic Area (EEA), however, if this is necessary, checks will be made to ensure an adequate level of protection for that information and consent will be sought from those affected.

11. School Specific Issues

11.1. Consent

11.1.1. The School will always seek consent/parental consent for the following:

- Photographs/Recordings of children used in school publications, including those to be used in the local newspaper and letters. Consent will be required for each time a photograph is to be used
- Photographs/Recordings of children that are used internally by the school, for school projects. Consent will be sought at the start of each school year
- 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. The School will accept consent that has been actively communicated in writing or by other means. The School will not infer consent from a non-response to a communication, for example from a parent's failure to return or respond to a letter.

[4] E.g. USB Memory Sticks, CD's, external hard drives, etc

11.2. CCTV

The School utilises CCTV as a means of security. CCTV footage will feature personal data, therefore the School makes sure that pupils, 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 pupils' 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. School Plays
The Data Protection Act does not prevent parents from capturing their child's performance on camera or video as these instances would be for personal/family use only and therefore the Act does not apply.

11.5. Biometric Data
Biometric data is personal data and must be processed according to the principles of the Data Protection Act 1998. 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.

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 Finance and Business Manager unless the breach relates directly to the Finance and Business Manager, 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 enquires regarding this policy or Data Protection in general should be referred to the Finance and Business Manager 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 the Data Protection Act 1998.