Data Protection Policy

1. Introduction

1.1. Hartmore School is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

1.2. This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees.

1.3. During the course of our activities we, Hartmore School, will process personal data (which may be held on paper, electronically, or otherwise) about our staff and we recognise the need to treat it in an appropriate and lawful manner, in accordance with the General Data Protection Regulation May 2018 (GDPR).

1.4. This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Definitions

2.1. "Personal Data" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

2.2. "Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

2.3. "Criminal Records Data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data Protection Principles

3. The school processes HR-related personal data in accordance with the following data protection principles:

3.1. The school processes personal data lawfully, fairly and in a transparent manner.

3.2. The school collects personal data only for specified, explicit and legitimate purposes.

3.3. The school processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.

3.4. The school keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

3.5. The school keeps personal data only for the period necessary for processing.

3.6. The school adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

3.7. The school tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

3.8. Where the school processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

3.9. The school will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

3.10. Personal data gathered during the employment, worker, contractor or volunteer relationship, apprenticeship or internship is held in the individual's personnel file in hard copy and electronic format on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

3.11. The school keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4. Fair & Lawful Processing

4.1. Hartmore School will usually only process your personal data where you have given your consent or where the processing is necessary to comply with our legal obligations. In other cases, processing may be necessary for the protection of your vital interests, for example to pay you, monitor your performance and to confer benefits in connection with your employment, for our legitimate interests or the legitimate interests of others. The full list of conditions is set out in the GDPR.

4.2. We will only process "sensitive personal data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions, where a further condition is also met. Usually this will mean that you have given your explicit consent, or that the processing is legally required for employment purposes.

4.2.1. The full list of conditions is set out in the GDPR.

5. How We Are Likely to Use Your Data

5.1. Hartmore School may process sensitive personal data relating to staff including, as appropriate:

- Information about an employee's physical or mental health or condition, in order to monitor sick leave and take decisions as to the employee's fitness for work
- The employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation
- in order to comply with legal requirements and obligations to third parties
- For recruitment decision purposes, seeking references and other pre- employment checks such as Criminal Records checks (DBS)

5.2. Hartmore School will only process personal data for the specific purpose or purposes notified, or for any other purposes specifically permitted by the GDPR.

6. Adequate Relevant & Non-Excessive Processing

6.1. Personal data will only be processed to the extent that it is necessary for the specific purposes notified to the employee.

7. Accurate Data

7.1. Hartmore School will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

8. Data Retention

81.1. Hartmore School will not keep your personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, please contact HR Department.

9. Processing in Line with Your Rights/Subject Access Request

9.1. As a data subject, individuals have a number of rights in relation to their personal data.

Subject Access Requests

9.2. Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

- Whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual
- To whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers
- For how long his/her personal data is stored (or how that period is decided);
- His/her rights to rectification or erasure of data, or to restrict or object to processing;
- His/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights
- Whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

9.3. We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise. If the individual wants additional copies, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

9.4. To make a subject access request, the individual should send the request to the HR Manager at Head Office. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

9.5. The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three-months of the date the request is received. The organisation will write to the individual within one-month of receiving the original request to tell him/her if this is the case.

9.6. If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it

10. Other Rights

10.1. Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- Rectify inaccurate data
- Stop processing or erase data that is no longer necessary for the purposes of processing
- Stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data)
- stop processing or erase data if processing is unlawful
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data

10.2. To ask the organisation to take any of these steps, the individual should send the request to the HR Manager at Head Office

11. Data Security

11.1. Hartmore School will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

11.2. Hartmore School have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3. Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

12. Providing Information to Third Parties

12.1. Hartmore School will not disclose your personal data to a third party without your consent unless we are satisfied that they are legally entitled to the data. Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

13. Breaches of This Policy

13.1. If you consider that this Policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager or senior member of staff. Any breach of this policy will be taken seriously and may result in disciplinary action.

13.2. If the organisation discovers that there has been a breach of HR-related , personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

13.3. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

14. Individual Responsibilities

14.1. Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.

- Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.
- Individuals who have access to personal data are required:
- To access only data that they have authority to access, and only for authorised purposes
- Not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction)
- Not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- Not to store personal data on local drives or on personal devices that are used for work purposes
- Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice

15. Training

16.1. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

16. Complaints

16.1. If you wish to make a complaint regarding breach of data protection, please contact the Information Commissioner on 0303 123 1113 or ico.org.uk/concerns.

17. Policy Review

17.1. This policy will be reviewed annually. It was written in January 2019 and will be reviewed in July 2020.