Data Protection Policy

Version 1

October 2018

HARDWICK HOUSE

Date reviewed	Version	Author
09/10/2018	1	LM

ACKNOWLEDGEMENT TO **FIFTH SQUARE LTD**

This document has been produced from a template provided under license by Fifth Square Ltd. Hardwick House School has used the template document in part and attributes full acknowledgement to Fifth Square Ltd.

The information contained in this document represents the current view of the author on the issue discussed as of the date of publication and is subject to change without notice. In the absence of any specific provision, this document has consultative status only. The Author shall not be liable for technical or editorial errors or omissions contained herein, although it has used reasonable endeavors to ensure accuracy and correct understanding.

Statement

The Directors of Hardwick House School are committed to compliance with all relevant UK and EU laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information Hardwick House School collects in accordance with the General Data Protection Regulation (GDPR).

To that end, the School's Data Protection Task Force have developed, implemented, will maintain and continuously improve management systems for documenting personal information at Hardwick House School. This policy will be reviewed annually to review its effective operation.

1 General Data Protection Regulation (GDPR)

1.1 The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive.

1.2 Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.3 Hardwick House School's objectives for the personal data management system are:

- that it should enable the organisation to meet its own requirements for the management of personal information
- that it should support organisational objectives and obligations
- that it should impose controls in line with Hardwick House School's acceptable level of risk
- that it should meet applicable regulatory, contractual and/or professional duties including compliance with statutory obligations related to employment, education and safeguarding.
- that it should protect the interests of individuals and other key stakeholders.

1.4 Hardwick House School is committed to complying with data protection legislation and good practice, including:

- collecting only the minimum personal information required for these purposes and not processing excessive personal information
- processing personal information only where this is strictly necessary for legitimate organisational purposes such as job applications
- adhering to the Data Protection Principles as outlined in section 3
- providing clear information to individuals about how their personal information will be used and by whom
- maintaining an inventory of the categories of personal information processed by Hardwick House School
- the application of the various exemptions allowable by data protection legislation
- developing and implementing a personal information management system to enable the policy to be implemented
- where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of Hardwick House School's personal information management system
- the identification of workers with specific responsibility and accountability for the personal information management system (the Data Protection Task Force)

2 Responsibilities

2.1 Hardwick House School is a data controller under the GDPR and is registered with the ICO.

2.2 The Directors and all those in managerial or supervisory roles throughout Hardwick House School are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.

2.3 The Data Protection Task Force is accountable to the Directors of Hardwick House School for the management of personal information and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- development and implementation of the personal information management system as required by this policy
- security and risk management in relation to compliance with the policy

2.4 A Data Protection Task Force, who the Directors consider to be suitably qualified and experienced, has been appointed to take responsibility for Hardwick House School's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the organisation complies with the GDPR.

2.5 The Data Protection Task Force have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees seeking clarification on any aspect of data protection compliance.

2.6 Compliance with data protection legislation is the responsibility of all members of Hardwick House School who process personal information.

2.7 Members of Hardwick House School are responsible for ensuring that any personal data supplied by them, and that is about them, is accurate and up-to-date.

3 Data Protection Principles

Hardwick House School holds personal data on students, staff and other individuals such as visitors and contractors. In each case, the personal data must be treated in accordance with the data protection principles.

3.1 Principle One: Personal data must be processed lawfully, fairly and transparently.

Please see Hardwick House School's relevant privacy policy. The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the data subject in an intelligible form using clear and plain language.

3.1.b The specific information that must be provided to the data subject must as a minimum include:

- the identity and the contact details of the controller and their representative
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the period for which the personal data will be stored
- the existence of the rights to request access, rectification, erasure or to object to the processing
- the categories of personal data concerned
- the recipients or categories of recipients of the personal data, where applicable
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data
- any further information necessary to guarantee fair processing

3.2 Principle Two: Personal data can only be collected for specified, explicit and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of Hardwick House School's GDPR registration.

3.3 Principle Three: Personal data must be adequate, relevant and limited to what is necessary for processing. The Data Protection Task Force are responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

3.3.b All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the appropriate member of the Data Protection Task Force.

3.3.c The Data Protection Task Force will ensure that, on an annual basis, all data collection methods are reviewed by internal audit methods to ensure that collected data continues to be adequate, relevant and not excessive.

3.4 Principle Four: Personal data must be accurate and kept up to date.
Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

3.4.b The Data Protection Task Force are responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

3.4.c It is also the responsibility of individuals to ensure that data held by Hardwick House School is accurate and up-to-date.

34.d Employees and parents should notify Hardwick House School of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Hardwick House School to ensure that any notification regarding change of circumstances is noted and acted upon.

3.4.e On at least an annual basis, the DP Leader will review all the personal data maintained by Hardwick House School, by reference to the Data Inventory Map, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed.

3.4.f The Data Protection Task Force is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information, the information is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.

Principle Five: Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing. Where personal data is retained beyond the processing date, it will be minimised/encrypted/pseudonymised in order to protect the identity of the data subject in the event of a data breach.

3.5.b Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

3.5.c The Data Protection Task Force must specifically approve any data retention that exceeds the retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

Principle Six: Personal data must be processed in a manner that ensures its security. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

3.6.b Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data. The transfer of personal data outside of the EU is prohibited unless specified safeguards or exceptions are applied that take into account the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant legislation
- codes of practice and international obligations; and
- the security measures that are to be taken in regard to the data in the overseas location.

3.7 The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR. Specifically, controllers are required

to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs (Data Processing Impact Assessment) where applicable, comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

4 Personal Data

4.1 Definitions

Personal data – any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.2 Hardwick House School often collects sensitive data for legitimate purposes relating to pupils, their parents or guardians, employees, visitors, volunteers, applicants and contractors. These purposes are explained within the Data Privacy Notices.

4.3 The objection to any use of personal data should be communicated to the Data Protection Task Force in writing, which will also be acknowledged in writing. If the objection to the use of personal data cannot be maintained, then a written explanation will be given stating why Hardwick House School cannot comply with the request.

5 Security

5.1 All Employees are responsible for ensuring that any personal data which Hardwick House Schools holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Hardwick House School to receive that information and has entered into a confidentiality agreement.

5.2 All personal data should be accessible only to those who need to use it and are authorised to do so. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with the companies access control procedures and/or stored on (removable) computer media which are encrypted.

5.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of Hardwick House School. All Employees are required to enter into

an Acceptable Use Agreement before they are given access to organisational information of any sort.

5.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation.

5.5 Personal data may only be deleted or disposed of in line with the data retention procedures. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

5.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

6 Data Subject's Rights

6.1 Data subjects have the following rights:

- To make subject access requests (see section 8) regarding the nature of information held on them or their children and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To erasure if there is no longer a legitimate reason for Hardwick House School to keep the data.
- Not to have significant decisions that will affect them taken solely by an automated process, and the right to object to any automated profiling without consent.
- To take action to rectify, block or destroy inaccurate data including to exert the right to be forgotten.
- To request the ICO to assess whether any provision of the GDPR has been contravened.
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

7 Consents

7.1 Hardwick House School understands 'consent' to mean that it has been explicitly and freely given, specific, informed and is unambiguous. The consent of the data subject can be withdrawn at any time.

7.2 Hardwick House School understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them.

7.3 In most instances consent to process personal and sensitive data is obtained routinely by Hardwick House School using standard consent documents e.g. when a new member of staff signs a contract of employment or when a new student joins the school.

7.4 Where Hardwick House School provides services to children, then parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16.

8 Rights of Access

8.1 Data subjects have the right to access any personal data (i.e. data about them) which is held by Hardwick House School in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect information obtained from third-party organisations about that person, including references.

8.2 A Subject Access Request (SAR) should be made in writing to the Directors of Hardwick House School. Hardwick House School will ensure that its response to the subject access request complies with the requirements of the GDPR Regulation. Hardwick House School might ask for more clarification on the data required. All files will be reviewed by the Data Protection Task Force before access to the data is provided.

8.3 In some instances, we might not be able to share information with you where it includes personal data relating to a third party, or for contractual, legal, regulatory or safeguarding reasons.

9 Disclosure of Data

9.1 Hardwick House School must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police.

9.2 All Employees should exercise caution when asked to disclose personal data held on another individual to a third party and may be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Hardwick House School business.

9.3 The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard
- prevention or detection of crime including the apprehension or prosecution of offenders
- assessment or collection of tax duty
- discharge of regulatory functions (includes health, safety and welfare of persons at work)
- to prevent serious harm to a third party
- to protect the vital interests of the individual, this refers to life and death situations.

As a school, we have a legal obligation to share certain types of data with the DfE, local authorities, and other third parties, e.g. support services.

9.4 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Directors.

10 Retention and Disposal

10.1 Personal data may not be retained for longer than it is required (or for the time set out in the relevant Privacy Notice). Once a member of staff has left Hardwick House School it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. Hardwick House School's data retention and data disposal procedures will apply in all cases.

10.2 Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal procedure.

11 Complaints and Breach

11.1 Data Subjects who wish to complain to Hardwick House School about how their personal information has been processed may lodge their complaint directly with a member of the Data Protection Task Force. They will need to be shown the relevant Privacy Notice explaining fair processing.

11.2 Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the Directors. The right to do this should be included in the GDPR section of Hardwick House School's Complaints Procedure.

11.3 The policy applies to all Employees (and third parties) of Hardwick House School such as outsourced suppliers. Any breach will be dealt with under Hardwick House School's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

11.4 Any suspected breach or non-compliance of the GDPR including of the data protection principles should be reported immediately to the Data Protection Task Force who will then assess the breach for risk to data subjects. Any breach of personal information which places an individual at risk must be reported by Hardwick House School to the Information Commissioner's Office within 72 hours of being reported.

12 Review

12.1 The Data Protection Task Force is responsible, each year, for reviewing the details of notification, in light of any changes to Hardwick House School's activities (as determined by changes to the Data Inventory Map and the management reviews) and to any additional requirements identified by means of data protection impact assessments.