Data Protection Policy

The Gryphon Trust

Approved by:		**Date:**
Implemented On:	25th May 2018	
Last Reviewed:	12th April 2018	
Next review due by:	5th April 2020 (or when the UK Data Protection Bill is enforced, whichever is earlier)	

Contents

.....

1. Introduction

The GDPR, General Data Protection Regulation, is replacing the Data Protection Act 1998 on 25th May 2018. This affects The Gryphon Trust as we process personal data about staff, students, parents and suppliers.

Our Trust aims to ensure that all data collected about our schools staff, pupils, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) 2018.

This policy applies to all data, regardless of whether it is in paper or electronic format.

The GDPR defines “personal data” as information relating to an identified or identifiable natural person.

2. Legislation and guidance

This policy meets the requirements of the General Data Protection Regulation, and is based on guidance published by the Information Commissioner’s Office and model privacy notices published by the Department for Education.

This policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Special Category Data	Data such as: • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Genetics • Biometrics
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Data Protection Officer (DPO)	The person or organization that's responsible for ensuring and encouraging compliance for the data controller
GDPR	The General Data Protection Regulation

4. The Data Controller

Our Trust processes personal information relating to pupils, staff, parents, suppliers and visitors, and, therefore, is a data controller. Our Trust delegates the responsibility of data controller to Miss S. Milligan, IT Manager of The Arnewood School, contactable at data@thegryphontrust.org or on 01425 625 432.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually, registration reference Z2600946.

5. Data Protection Principles

This policy aims to ensure The Gryphon Trusts complies with the GDPR. The GDPR sets out the following principles with which all of the personal data we hold must comply. All personal data must be:

- Processed lawfully, fairly, and in a transparent manner relating to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. The Rights of Data Subjects

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

7. Roles and responsibilities

The governing board has overall responsibility for ensuring that the school complies with its obligations under the General Data Protection Regulation.

Day-to-day responsibilities rest with The Data Protection Officer in the Trust, or the Trust CEO in the DPO's absence. The DPO will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

Staff must report a breach of personal data to the Data Protection Officer immediately.

N.B. Staff should note that failing to report a data breach will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Any member of staff or student who deliberately gains or attempts to gain unauthorised access to personal data on any data subject or discloses such data to any third party may be disciplined in accordance with school procedures.

8. Subject access requests

Under the GDPR, pupils have a right to request access to information the school holds about them. This is known as a subject access request (SAR). The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

Subject access requests must be submitted in writing to the Data Protection Officer, either by letter or email. Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child
- Any information regarding an exam script or for exam marks before they are officially announced
- Any information the teacher has solely for their own use

Subject access requests for all or part of the pupil's educational record will be provided within 30 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request within the 30 days.

SARs are provided free of charge unless when a request is manifestly unfounded or excessive, particularly if it is a repetitive request, then a reasonable fee will be charged.

9. Parental requests to see the educational record

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, in addition to the upcoming UK Data Protection Bill, generally regards children aged 13 and above as mature enough to understand their rights and the implications of a subject access request.

As a multi academy trust, The Gryphon Trust is able to define a process for data requests in regards to parents/carers requesting to see their child's data. In most instances, if parents/carers request to see personal data on their child we will process this request without the consent of the child until the child reaches Sixth Form. At this stage, the decision to release the data lies with the pupil concerned.

Please note every individual subject access request on behalf of a pupil is undertaken in a bespoke manner, taking all details into consideration and it may be that the pupil in question is required to give their consent if there are justified reasons for this. In all instances the pupil will be informed of a Subject Access Request received by the Gryphon Trust that concerns them.

Therefore, most subject access requests from parents/carers of pupils at our schools may be granted without the express permission of the pupil until the student reaches Sixth Form (year 12 and upwards).

10. Storage & Secure Processing of Records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office or archive areas
- Passwords that are at least 8 characters long containing letters, symbols and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Data is kept for only as long as necessary and will be rectified without delay if found to be inaccurate
- Accuracy of data will be checked when it is collected and at regular inspections thereafter.
- The Trust will undertake Data Protection Impact Assessments for any and all new projects and processing of any personal data
- All emails containing personal data will be marked 'confidential'
- Where personal data is printed or filled out on a hardcopy form it should be passed directly to the recipient wherever possible
- No personal data is to be stored on any device personally belonging to an employee, pupil or governor
- All personal data stored electronically will be backed up daily with backups stored offsite with the DPO. All backups should be encrypted.
- No personal data should be stored on a mobile device, whether such device belongs to the Trust or personally, without formal written approval of the Data Protection Officer and is entered onto the Gryphon Trust Data Register. In the event of such approval, the data must not be kept for longer than is absolutely necessary
- If personal data is visible on a computer screen and the computer in question is to be left unattended for a period of time, the user must lock the computer and screen
- Where personal data is used for marketing purposes, it shall be the responsibility of the Marketing Officer to ensure that the appropriate consent is obtained from Data Subjects, whether directly or via a third-party supplier.
- Under no circumstances must passwords be written down or shared between any employees, contractors, or other parties working on behalf of the Gryphon Trust. IT staff do not have access to passwords.
- All software, including applications and operating systems, shall be kept up to date and IT staff shall be responsible for installing any and all updates. No software may be installed on a Trust owned computer or device without the prior approval of the IT department at the corresponding school.
- All employees, agents, contractors or other parties working on behalf of the Trust shall be responsible for their individual responsibilities and the Gryphon Trust's responsibilities under the GDPR and under this Policy, and shall be provided with appropriate training and documentation.
- Methods of collecting and storing personal data shall be regularly evaluated and reviewed.
- Where any agent, contractor or other third party working on behalf of the Trust are handling personal data, they shall comply with conditions under this Policy, if they fail to, that party shall indemnify and exclude the Trust against any costs, liability, damages, loss or claims that may arise out of their failure.
- Any cloud storage is located within Europe, opting to be stored within the UK where applicable, and is sufficiently secured under ISO27001, Cyber Essentials and other secure processes.
- The Gryphon Trust may transfer personal data outside of the EEA (transfer includes making available remotely) only if there is at least the security of the data to at least the level the GDPR ensures. Any occurrences will be listed in the Gryphon Trust Privacy Notice.

- Ensure Data Sharing Agreements or updates to contracts covering their GDPR responsibilities are in place with all third parties and suppliers including the government, Hampshire and Social Services

11. Data Breaches

All personal data breaches must be reported to the Data Protection Officer immediately.

If a personal data breach is likely to result in a risk to the rights and freedoms of the Data Subjects, the DPO must ensure that the ICO and the affected Data Subjects are informed of the breach without undue delay

12. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic devices/records.

The Gryphon Trust shall not keep any data for any longer than is necessary in light of the purpose for why that personal data was originally collected, held and processed.

In the event that a request for erasure is made by a data subject, the Trust has the right to refuse the erasure if there are legitimate interests for the Trust to still require the data held. If data is to be erased in response to a data subject's request, all third parties that also hold their data will also be contacted and informed of the erasure request, unless this is impossible or would require disproportionate efforts to do so.

Whilst a request for erasure is being processed, the Data Subject's personal data will cease from being processed, unless the Trust's legitimate grounds for processing overrides the data subject's interests, rights and freedoms.

For full details of our Trust approach to data retention, including retention periods for all data types held, please refer to our Gryphon Trust Data Retention Schedule.

13. Training

Our staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

Any temporary workers will receive details of the Trust's Data Protection Policy and will be asked to sign a confidentiality clause for any personal data they may process as part of their contract.

14. Monitoring arrangements

The Data Protection Officer is responsible for monitoring and reviewing this policy.

The Data Protection Officer checks that the school complies with this policy by, among other things, reviewing school records every six months.

This document will be reviewed when the General Data Protection Regulation comes into force, followed by the new UK Data Protection Bill being enforced, and then **every 2 years**.

At every review, the policy will be shared with the governing board.

15. Links with other policies

This data protection policy is linked to the 'Gryphon Trust Privacy Policy', the 'Gryphon Trust Data Retention Schedule' and the freedom of information publication scheme.

16. Complaints

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 (the statutory regulator).

17. Contacts

If you have any enquires in relation to this policy, please contact Miss Milligan, The Data Protection Officer who will also act as the contact point for any subject access requests on 01425 625 432 or data@thegryphontrust.org

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.