General Data Protection Regulation (GDPR) Policy

Mission Statement

The Unity of Titchmarsh and Warmington Schools ('The Unity') aims to provide a caring, secure and enriching experience; each child is encouraged to develop strong personal, academic, physical and creative skills for lifelong learning.

The Unity collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the schools. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the schools comply with their statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing and Privacy Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations (2018), and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times and the GDPR builds upon these:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The GDPR is based on the following principles (from Article 5) – that personal data is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) 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."

General Statement

The Unity is committed to maintaining the above principles at all times. Therefore the Unity will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Lawful, Fair and Transparent Data Processing

We will ensure, through compliance with the GDPR principles, that our data processing is lawful, fair and transparent. Privacy notices will be available on the schools' websites and we will contact you when we request data for your permission, why we need the data, what we will do with it and how it will be used.

We have undertaken data audits to ensure that the data we collect is adequate and relevant to the needs of the school. We will also ensure that we regularly contact you to keep our data up to date.

We will undertake Privacy Impact Assessments where we are using personal data in a new way and will ensure that privacy notices are amended accordingly.

We will also ensure that consent is 'freely given, informed, specific and explicit' so that when we ask for consent to use and process data, the purpose will be clear for each item being requested.

Security

It is Unity policy that all data is securely held and we are in a process of ensuring that data, in whatever form, is secure. Any breach of security will be reported as a data breach. The privacy notices issued by the Unity clearly outline the use of data and who it is shared with.

Security advice for staff is also detailed in the Unity Code of Conduct.

Rights of Data Subjects

These are detailed in the Unity Privacy Notices. We will also keep you informed of the data requested through data returns and will write to you to seek your permission when new data is required, giving the reason for the request, along with how it will be stored, shared (if applicable) and disposed.

You also have the right to make a subject access request. The process for this is detailed in Appendix 1. From this, you have a right to request rectification or erasure of personal data, other than that held for statutory reporting or public interest reasons.

Data Portability

The Unity's Fair Processing and Privacy Notices explain the situations where data will be shared and/or moved. This is most likely to be a transfer to another school as part of an in-year transfer or at the end of Year 6 where pupils move to secondary school. Please see our notices for further details.

Data Protection Measures

It is Unity policy to take all reasonable steps to ensure data protection is in place. All staff and governors will have received training in GDPR measures and will be clear of the expectations and consequences of a data breach. All PCs will be subject to password protection and will not be left unattended, with additional expectations of a time-out facility to prevent access to data. Any data taken off-site must be on an encrypted memory stick which the Unity will provide.

The Unity Code of Conduct and related policies/job descriptions will detail expectations and responsibilities for staff. Any breach of these will be dealt with according to the relevant policies. See Appendix 2 for further details.

Data Breach Notification

Where there is a data breach, this will be reported to the relevant Data Protection Officer who will take appropriate action in line with school procedures, including reporting to the ICO where necessary.

Data Retention and Disposal

These will comply with the guidance in the Information Management Toolkit for Schools.

Complaints

Complaints will be dealt with in accordance with the Unity's Complaints Policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 4 years. The policy review will be undertaken by the Executive Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Louise Guy (01832) 280420 or Mel Skerritt (01832 732874) who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745

Associated Policies:

Retention Guidelines (Information Management Toolkit for Schools)
ICO Guidelines
Whistleblowing Policy
Staff Code of Conduct
E-Safety and Acceptable Use Policy
Fair Processing and Privacy Notices

Appendix 1

The Unity of Titchmarsh and Warmington Schools

Procedures for responding to subject access requests made under the Data Protection School on Act 1998 and GDPR (2018).

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.
1. Under the General Data Protection Regulations (2018), any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (England) Regulations 2006.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Executive Headteacher**.** If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may not make a charge for the provision of information under GDPR.

5. The response time for subject access requests, once officially received, is 20 school days or 60 school days for more complex requests **(whichever is shorter)**. However the 20 days will not commence until after clarification of information sought. As the schools are only operational for part of the year, it may not be possible to gain the information within the

timeframe, therefore, applicants must bear this in mind prior to a request close to a major school holiday.

6. The GDPR allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 20 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact Louise Guy (01832) 280420 or Mel Skerritt (01832 732874) in the first instance.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone.

Appendix 2

The Unity of Titchmarsh and Warmington Schools Stakeholder Responsibilities:

School Staff (including Executive Headteacher, Teaching and Support Staff)

All staff should ensure:

- They are familiar with the requirements of safe data handling and the GDPR;
- They password-protect any devices they use that can be accessed by others;
- They only save data to be taken out of school on encrypted data sticks;
- They are mindful about safe use of data: ensuring a clear desk policy, ensuring PCs or other equipment are not left unattended so that others can access information;
- That key information is locked away;
- That, if working from home, that data is not stored on shared devices that can be easily accessed by non-school staff;
- That displays and other information visible cannot lead to the breaching of personal data;
- That they ensure that confidential documents are sent with a password protect facility and any confidential discussions are held in suitable areas of the school.

Staff are reminded that they should always act professionally when using any ICT equipment and that all school-based information is potentially available on request.

Governors

All governors should ensure:

- They are familiar with the requirements of safe data handling and the GDPR;
- They password-protect any devices they use for governor business that can be accessed by others;
- They only save data to be taken out of school on encrypted data sticks or have appropriate security on portable devices;
- They are mindful about safe use of data: that, if working from home, that data is not stored on shared devices that can be easily accessed by non-school staff;
- That displays and other information visible cannot lead to the breaching of personal data;
- That they ensure that confidential documents are sent with a password protect facility and any confidential discussions are held in suitable areas of the school.

Visitors

All visitors should ensure:

- They are familiar with the requirements of the GDPR via a school leaflet;
- They provide relevant identification when arriving at the school.

Staff are reminded that displays and other information visible should not lead to the breaching of personal data.