Thurlbear CE VA Primary School

DATA PROTECTION POLICY

(This policy includes information on: Subject Access Requests, Freedom of Information, Data Breach Reporting and Data Retention procedures)

Data Processing Officer: Ian Gover - dposchools@somerset.gov.uk

School Data Processing Lead: Jo Moore - jmoore@educ.somerset.gov.uk

The policy was approved by Governing body on: 22/05/2018

Signature of Chair of Governors: _____

The next review date is: Sept 2019

Version Control

Version	Author(s)	Date Produced	Amendments
1.0	Jo Moore	24/04/18	

Contents

Introduction

Thurlbear CE VA Primary School has a statutory requirement to keep and process certain information about its staff, pupils and other users in accordance with its legal obligations under General Data Protection Regulations (GDPR).

The School sometimes has to share this information about pupils, staff and other users because we have a legal and statutory duty to do so.

The school will comply with the data protection principles which are set out in Data Protection regulations and other laws.

This policy is in place to ensure all staff and governors are aware of their responsibilities and how the school complies with the core principles of GDPR.

The Data Controller and other roles

The School, as a body, is the Data Controller.

The School has identified a designated Data Protection Officer (DPO). The DPO for this school is Ian Gover dposchools@somerset.gov.uk. To find out more about the role of the DPO see Appendix A.

Other day to day matters will be dealt with by The Data Protection Lead (DPL) and the Senior Leadership Team. The DPL for this school is the School Business Manager jmoore@educ.somerset.gov.uk. To find out more about the role of the DPL see Appendix B.

Responsibilities of the School

The school is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors. This implies that the school will:

a) register with the Information Commissioners Office (ICO);
b) place on its website Privacy Notices regarding the personal data held about them and the reasons for which it is processed. More information about Privacy Notices can be found at the end of the document.
c) obtain consent of the data subject for the non-statutory use of personal data such as the use of images and names in publicity materials and where consent is given a record will be kept documenting how and when consent was obtained.
d) keep an up to date Data Asset Audit which lists all known uses of personal data in the school;
e) verify that all systems that involve personal data or confidential information will be examined to see that they meet the Data Protection regulations;
f) inform all users about their rights regarding data protection;
g) provide training to ensure that staff know their responsibilities;
h) monitor its data protection and information security processes on a regular basis, changing practices if necessary.

Responsibilities of Staff

All staff are responsible for checking that any information that they provide to the School is accurate and up to date.

All staff are responsible for ensuring that any personal data they use in the process of completing their role:

a) is not in the view of others when being used;
b) is kept securely in a locked cabinet when not being used;
c) is stored on a password protected local hard or network drive;
d) if kept on removable storage (a laptop, tablet, USB memory stick) approved by the school and that this is password protected and encrypted. The data held on these devices must be backed up regularly and this is the responsibility of the individual;
e) is not disclosed or shared with any unauthorised third party;
f) is assessed and approved by the DPL or Senior Leadership Team or with advice from the DPO if used within an app, webservice or other application.

The school takes its duties under the GDPR very seriously and any unauthorised disclosure may result in disciplinary action.

Responsibilities of Parents/Guardians

The school will inform the Parents/Guardians of the importance of the personal data the school uses and the importance of keeping this data up to date.
Reminders will be via newsletters and on the school website. Parents/Guardians will be requested to complete an annual data collection sheet (with the return of this document being recorded). The School will place on its website Privacy Notices regarding the personal data held about them and the reasons for which it is processed.

Other permissions will also be sought regarding matters of non-statutory use of personal data such as the use of images and names in publicity materials on induction or when required. The returns to these permissions will be recorded and exemptions communicated to staff.

Rights to Access Information

All people having personal data stored by the school have the rights to:

a) obtain from the school confirmation if personal data concerning him or her (or their child) is being processed;

b) Where this is the case, have a copy of the personal data and the following information:

(i) the purposes of the processing;
(ii) the third parties that the data will be shared with;
(iii) the period for which the personal data will be stored;

(iv) the existence of the right to request from the school to correct, erase or restrict processing of personal data if the data can be proved to be incorrectly held;
(v) the right to lodge a complaint with a supervisory authority;
(vi) where the personal data are not collected from the data subject, any available information as to their source.

c) if exemptions are placed on any of the data above, because of safeguarding or other issues, the existence of this data will be declared.

The School will place on its website Privacy Notices regarding the personal data held about them and the reasons for which it is processed.

Access to the data is called a Subject Access Request. Any person who wishes to exercise this right (or their parental right) should make a request in writing and submit it to the Head teacher or the Chair of Governors. The process for dealing with these requests is outlined in Appendix C.

The School aims to comply with requests for access to personal information as quickly as possible and in accordance with advice from the ICO and other professional agencies.

Freedom of Information Requests

Freedom of Information requests are requests from any member of the public about processes, policies and other non-personal information about the school. These requests will always be processed and the rights of individuals (within Data Processing Regulations) not to be identified respected while maintaining legal responsibilities within the Freedom of Information Act.

The process for dealing with Freedom of Information requests is given in Appendix D.

Data Breaches

If there is a Data Breach the school will inform the DPO who will then advise on any actions.

Any Data Breaches will be recorded, comprising the facts relating to the personal data breach, its effects and the remedial action taken as shown in Appendix E.

If there are risks to the individual the school will communicate the breach to the data subjects.

In the case of a personal data breach where there is a high risk to the rights and freedoms of the data subject, the DPO/School will without undue delay and not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.

Data Retention Policy

The school has responsibilities under the Data Protection Principles to keep data only for as long as we need to.

In respect of the length of time that schools should keep the data the school will follow the advice from the IRMS using their Records Management Toolkit for schools.

If paper is due to be destroyed it will be cross-cut shredded either school or by a commercial company.

If data is held on electronic devices then these will be deleted in line with the advice from the ICO.

A record should be kept of the data destroyed and/or the certificate of destruction issued by a third party.

Reporting policy incidents

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data should raise the matter with the Head Teacher or Chairman of Governors.

Monitoring and Evaluation

This policy will be monitored and reviewed in line with the school's policy review procedure.

Useful Information

Privacy notices: https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

ICO: https://ico.org.uk/for-the-public/online/deleting-your-data/

Appendix A – Roles of Data Processing Officer

Purpose

The Data Protection Officer (DPO) is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee and verify the school's data protection processes and advise the school on best practice.

Within each school there will be a Data Protection Lead (DPL), who maintains contact with the DPO and is responsible for assisting in monitoring with compliance and verifies the school's data protection practices on a day to day basis.

Data Protection Officer Responsibilities

To:

- advise the school about their obligations under current data protection regulations;
- support the DPL in developing a joint understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist, in cooperation with the DPL, with the monitoring of the school's compliance with data protection law, by:
    - collecting information to identify data processing activities;
    - analysing and checking the compliance of data processing activities;
    - informing, advising and issuing recommendations to the school;
    - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the DPL in making sure that the school's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - co-ordinating staff training;
    - conducting internal data protection audits;
- advise on and assist the school with carrying out data protection impact assessments, if necessary;
- act as a contact point for the ICO, assisting and consulting it where necessary, including:
    - helping the ICO to access documents and information;
    - seeking advice on data protection issues;

- act as a contact point for individuals whose data is processed (for example, staff, pupils and parents), including:
    - responding with support from the DPL to subject access requests;
    - responding with support from the DPL to other requests regarding individuals' rights over their data and how it is used;
- take a risk-based approach to data protection, including:
    - prioritising the higher-risk areas of data protection and focusing mostly on these
    - advising the school if/when it should conduct an audit, which areas staff need training in, and what the DPO/DPL roles should involve.
- report to the governing board/board of trustees on the school's data protection compliance and associated risks;
- respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role;
- assist the DPL in maintaining a record of the school's data processing activities;
- work with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the DPL in fostering a culture of data protection throughout the school;
- work closely with other departments and services to ensure GDPR compliance, such as HR, legal, IT and security;
- work with the Senior Leadership team at the school to ensure GDPR compliance;
- assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

Tasks
From these responsibilities, isolated tasks should include:

- providing a model Data Protection Policy and assist in customising it for the school;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- providing advice on other associated policies and documents;
- providing materials and advice in completing a dynamic Data Asset Audit and assisting in its completion if necessary;
- collecting the Data Asset Audit on a yearly basis and checking for issues;
- providing training materials to allow the DPL to assist staff in keeping up to date with Data Protection issues;

- acting as the point of contact for SAR and FOI requests and supporting the school to provide the information as required;
- providing a Data Protection Audit on a 3 yearly rota basis and producing a report for Governors;
- providing telephone and email advice and support;
- providing regional training for the DPL and other staff;
- providing school based on-demand training either as part of the Ed Tech subscription or at cost.

Appendix B – Data Protection Lead Role

Data Protection Lead Responsibilities

To:

- verify that the school has registered with the ICO;
- support the DPO in advising the school about their obligations under current Data Protection regulations;
- support the DPO in developing an understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist, in cooperation with the DPO, with the monitoring of the school's compliance with data protection law, by:
    - collecting information to identify data processing activities;
    - analysing and checking the compliance of data processing activities;
    - informing, advising and issuing recommendations to the school;
    - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the DPO in making sure that the school's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - co-ordinating staff training;
    - conducting internal data protection audits;
- act as a contact point for the DPO in supporting individuals whose data is processed (for example, staff, pupils and parents), including:
    - responding with support from the DPO to subject access requests;
    - responding with support from the DPO to other requests regarding individuals' rights over their data and how it is used;
- assist the DPO in maintaining a record of the school's data processing activities providing this on a yearly basis to the DPO;
- assisting the DPO in working with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the DPO in fostering a culture of data protection throughout the school;
- work with the Senior Leadership team at the school to ensure GDPR compliance;
- assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- act as the point of contact with the DPO;
- assist in customising the Data Protection Policy for the school;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- provide advice on other associated policies and documents;
- providing materials and advice in completing a Data Asset Audit and assisting in its completion if necessary;
- supplying the DPO with the Data Asset Audit on a yearly basis;
- using the training materials provided by the DPO to assist the staff in keeping up to date with Data Protection issues.

Appendix C – Process for dealing with Subject Access Requests

On receiving a Subject Access Request or request for change or deletion of data the DPO or school will:

- inform the DPL in the school (and the Headteacher if necessary);
- record the details of the request, updating this record where necessary (see next page);
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- contact the DPO if clarity on the request is needed or procedure is needed;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **30 calendar days**, which can be extended by a further 2 months where the request is complex or where there are numerous requests.

Please note the time for processing a request for an Educational Record is **15 days**.

Appendix D – Process for dealing with Freedom of Information Requests (FOI)

On receiving a Freedom of Information Request, which must be made in writing, the DPO or the school will:

- inform the DPL in the school (and the Headteacher if necessary);
- record the details of the request, updating this record where necessary (see next page);
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- decide that if the material is already published or falls within an exemption;
- contact the DPO if clarity on the request is needed or procedure is needed;
- if data is not going to be published inform the requestor why this is not being released;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **20 working days**.

Appendix E – Data Breach

Every Data Protection Breach should be recorded. The process that should be followed is listed below:

- inform the DPL in the school (and the Headteacher if necessary);
- record the details of the breach, updating this record where necessary;
- contact the DPO if clarity on reporting the breach is needed and if necessary report to the ICO;
- identify the people whose data is accidentally released, inform them of the breach and the processes taken to rectify the situation;
- review why the breach took place and if future similar events can be avoided.