Abbas and Templecombe
Church of England Primary School
School Lane, Templecombe, Somerset, BA8 0HP
Head Teacher - Mr James Webb
Email – abbastemplecombe@educ.somerset.gov.uk
Phone – 01963 370481

DATA PROTECTION POLICY
(includes Subject Access and FoI procedures)

Version Number	2.1		
Author	James Webb		
Published	September 2018	Signed:	J. Webb
Review Date	January 2020		Data Processing Lead
Effective Date	September 2018	Date:	05/09/2018
Consultation	This Policy has been prepared in line with the guidance and procedures of the GDPR. It is broadly derived from Somerset eLIM's model policy.		

Introduction

- Abbas and Templecombe School needs to keep information about our pupils, staff and other users to allow us to follow our legal and statutory duties and to provide other services.
- Abbas and Templecombe School will comply with the data protection principles which are set out in the General Data Protection Regulation[i] and other laws.

The Data Controller and the Designated Data Controllers

- Abbas and Templecombe School, as a body, is the Data Controller.
- Abbas and Templecombe School has identified its designated Data Processing Officer (DPO) as Amy Brittan, who will deal with matters detailed in appendix A.
- Other day to day matters will be dealt with by The Data Protection Lead, which is the Headteacher.

Responsibilities of Abbas and Templecombe School

We are committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors.

This implies that:

a) All systems that involve personal data or confidential information will be examined to see that they meet the General Data Protection Regulations;
b) We will inform all users about their rights regarding data protection;
c) We will provide training to ensure that staff know their responsibilities;
d) We will monitor our 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.

For the purposes of this policy the school splits personal pupil data into two categories; sensitive and educational. Each type of data will be treated differently with sensitive data having additional restrictions placed upon it.

We define sensitive data as information that is highly personal to the child and could cause them harm if it was released to third parties; for example pupil information record (held on SIMs), safeguarding and inclusion information, etc. This type of data must be:

a) not in the view of others when being used;
b) kept securely in a locked filing cabinet or drawer when not being used;
c) be password protected both on a local hard drive and on a network drive that is regularly backed up;
d) if kept on a laptop, is password protected. The data held on these devices must be backed up regularly;
e) is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure or transgression of the above statements will usually be a disciplinary matter.

We define educational data as information that although personal to the child would not cause them harm if it was accidentally released to third parties; for example pupil assessment information, class lists, reward charts, marked work, etc. This type of data must be:

a) only on display if considered absolutely necessary (this will be identified as such in the data asset audit) otherwise this educational data should be kept in staffs desk draws or cupboards;
b) secured with a data sharing agreement for third party users, e.g. Accelerated Reader, Pupil Accet, etc.
c) kept out of sight of others if taken home by staff, e.g. to mark pupil books.

Responsibilities of Parents/Guardians

The school will inform the Parents/Guardians of the importance of (and how to make) any changes or deletions to personal data. This includes an annual data collection sheet, with the return of this document being recorded.

Other permissions will also be sought regarding matters of non-statutory use of personal data such as the use of images and use of names in publicity materials on induction, annually 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 as to whether personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information:
   (i) the purposes of the processing;
   (ii) the categories of personal data concerned;

(iii) the recipients or categories of recipient to whom the personal data have been or will be disclosed. In particular, recipients in third countries or international organisations;
(iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(v) the existence of the right to request from the school rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(vi) the right to lodge a complaint with a supervisory authority;
(vii) where the personal data is not collected from the data subject, any available information as to their source;
(viii) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

b) know where personal data is transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

c) have a copy of the personal data undergoing processing. For any further copies requested by the data subject, the school may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

d) obtain a copy referred to in paragraph c) shall not adversely affect the rights and freedoms of others.

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

All staff, parents and other users have a right to ask to view personal data being kept about them or their child called a Subject Access Request. Any person who wishes to exercise this right should make a request in writing and submit it to the Headteacher. The process for dealing with these requests is outlined in Appendix B.

The School aims to comply with requests for access to personal information as quickly as possible and in compliance with advice from the Information Commissioner's Office and other professional agencies. There may be an administration charge which will be stated once the enquiry is made.

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

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 G.

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 the ICO should be informed as soon as possible and **within 72 hours of notification**. Further investigation of the breach can take place after this notification in line with advice from the DPO and the ICO.

Data breaches are reported using the information found at these webpages:

- https://ico.org.uk/for-organisations/report-a-breach/
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

When reporting a breach, the Data Protection Act 2018 states that you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

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 about himself or herself or their child should raise the matter with the Head Teacher, in the first instance. Alternatively, they could contact the DPO directly.

Monitoring and Evaluation

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

Appendix A – Role of Data Processing Officer

According to Article 37(5), the DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

These are:

- to inform and advise the controller or the processor and the employees who are processing personal data, of their obligations pursuant to this Regulation;
- to monitor compliance with this Regulation, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested about the data protection impact assessment and monitor its performance, pursuant to Article 35;
- to cooperate with the supervisory authority (the ICO in the UK);
- to act as the contact point for the supervisory authority on issues related to the processing of personal data.

Appendix B – Process for dealing with Subject Access Request or request for change or deletion of data

On receiving a Subject Access Request or request for change or deletion of data (including parent contact numbers) the school will:

- inform the Data Protection Lead in the school;
- record the details of the request, updating this record where necessary;
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- make contact with 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 days, which can be extended by a further 2 months where the request is complex or where there are numerous requests.

Appendix C – Data Asset Audit

The school will document the personal data it stores.

This document will be a dynamic document and be the responsibility of the DPL assisted by the DPO.

It will be updated using the Privacy Impact Assessment forms completed by staff.

The document can be in any format but should contain information about the type of data held, why it is held, who it is shared with and any anticipated risks.

Appendix D – Staff Privacy Impact Assessment Form

Before the use of any new service that uses personal data, staff should fill in a Privacy Impact Assessment Form.

The Senior Leaders and/or the DPL, with advice from the DPO will then approve the use and the information be placed on the Data Asset Audit.

Privacy Impact Assessment Form

Privacy Impact Assessment (PIA) for:
Name of Service/Software/App

Data Protection Principles

- processing to be lawful and fair
- purposes of processing be specified, explicit and legitimate
- adequate, relevant and not excessive
- accurate and kept up to date
- kept for no longer than is necessary
- processed in a secure manner

Why we need a Privacy Impact Assessment – screening questions?
We need to complete this form because:

- the use involves the collection of new information about individuals;
- the use compels individuals to provide information about themselves;
- the information about individuals will be disclosed to organisations or people who have not previously had routine access to the information;
- we are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- we are using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition;
- the use results in you making decisions or acting against individuals in ways that can have a significant impact on them;
- the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private;
- the use requires you to contact individuals in ways that they may find intrusive.

Describe the service			
Describe the data collected and the possible uses of the data			
List of data held	Collection of data		
	Possible uses		
Identify the privacy, related risks and possible solutions To be discussed with the Data Protection Lead			
Privacy issue	Risk to individuals	DPA Risks	Possible Solutions
1.	•	•	•
2.	•	•	•
3.	•	•	•
4.	•	•	•
5.	•	•	•
6.	•	•	•
Sign off and notes			
Comments on risks	Processes that must be in place		
Contact point for future privacy concerns Data Protection Officer: dposchools@somerset.gov.uk Data Protection Lead: A Person - aperson@educ.somerset.gov.uk Date completed: 05/09/2018			

Appendix E – 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.

Subjects Access Requests are held by the Head Teacher.

Subject Access Request Record

Name of data subject: _____

Name of person who made request: _____

Date request received: ____/____/____

Contact DPO (dposchools@somerset.gov.uk) : ____/____/____

Date acknowledgement sent: ____/____ /____

Name of person dealing with request: _____

	Notes (Overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons and/or ask for proof
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, ask third parties to release external data. If data is supplied by another agency such as Psychology Service, you do not own the data.
Do you need to exempt/redact data?	If exempting/redacting be clear of your reasons Document name, data exempted/redacted, why.
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?

At all stages, your DPO or DPL will be able to provide you with advice.

Date request completed: ____/____/____
(within 30 days of request)

Signed off by: _____

Appendix F – Process for dealing with FoI Requests

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.

Freedom of Information requests are held by the Head Teacher.

Freedom of Information Request Record

Name of person who made request: _____

Date request received: ____/____/____

Contact DPO (dposchools@somerset.gov.uk) : ____/____/____

Date acknowledgement sent: ____/____ /____

Name of person dealing with request: _____

	Notes (Overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, then refer them to the correct agency
Do you need to exempt/redact data?	Could the data identify individuals Are any of the answers less than 5 people – use '5 or less including zero)? Are their commercial sensibilities?
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?

At all stages, your DPO or DPL will be able to provide you with advice.

Date request completed: ____/____/____
(within 20 days of request)

Signed off by: _____

Appendix G – 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 providing these details:

    - a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
    - the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
    - a description of the likely consequences of the personal data breach; and
    - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

- contact the DPO if clarity on reporting the breach is needed and if necessary report to the ICO;

    - either by phoning 0303123 1113
    - By filling in the form at:

https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc
and sending it to casework@ico.org.uk

- updating this record where necessary (see next page);

- 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.

Data Protection Breach records requests are held by the head Teacher.

Data Breach Record

Date: / /	**Person responsible for dealing with breach**				
Description of the nature of the personal data breach including, where possible:					
The categories and approximate number of individuals concerned					
The categories and approximate number of personal data records concerned					
A description of the likely consequences of the personal data breach					
A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects					
Reported by					
Phone/email sent to DPO dposchools@somerset.gov.uk	**y/n**	**Is this high risk?**	**y/n**	**Report to ICO**	**y/n**
Date reported to data subjects					
Notes					
Actions approved by		**Date**	**/ /**		

[i] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679