The Castle Partnership Trust
ACHIEVE | BELONG | PARTICIPATE

DATA PROTECTION POLICY

(Includes Subject Access, FoI, Data Breach Reporting and Data Retention Procedures)

May 2018

Data Processing Officer: Amy Brittan - dposchools@somerset.gov.uk

Data Processing Lead: Mrs A Crudgington (The Castle School) and Mr P Cox (Court Fields School).

Review date: Summer Term 2019

Contents

Introduction

The Trust needs to use information about students, staff and other users to allow us to follow our duties, and to provide other services with data that we have a legal, statutory or contractual right to process.

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

The Data Controller and Other Roles

The Castle Partnership Trust, as a body, is the Data Controller.

The Trust has identified its designated Data Protection Officer (DPO – see Appendix A).

Other day-to-day matters will be dealt with by The Data Protection Lead (DPL see Appendix B), The Headteacher/Head of School, Deputy Headteacher, and the Senior Administrator.

Responsibilities of the Trust

The Trust is committed to protecting and respecting the confidentiality of sensitive information relating to staff, students, parents and governors/directors. We will:

a) register with the Information Commissioners Office (ICO);
b) keep an up to date Data Asset Audit (See Appendix C) which lists all known uses of personal data in each school;
c) verify that all systems that involve personal data or confidential information will be examined to see that they meet the Data Protection regulations;
d) inform all users about their rights regarding data protection;
e) provide training to ensure that staff know their responsibilities;
f) 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 Trust 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 or locked room 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), is password protected and encrypted and the data held on these devices is backed up regularly;
e) is not disclosed to any unauthorised third party;

f) is assessed and approved by the Strategic Leadership Team (SLT) or the DPL with advice from the DPO (see Privacy Impact Assessment from Appendix D) if used within an app, webservice or other application.

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

Responsibilities of Parents/Guardians

The Trust will inform Parents/Guardians of the importance keeping their personal data up to date. This process will include an annual data collection sheet (with the return of this document being recorded) and reminders by email.

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 admission to each school, 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 Trust have the right to:

a) obtain from the Trust 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 Trust 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 is not collected from the data subject, any available information as to the 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 Trust will place on the school websites Privacy Notices[1] regarding the personal data held 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

[1] https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

to the Headteacher/Head of School or the Chair of Governors. The process for dealing with these requests is outlined in Appendix E.

The Trust 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 Trust. 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 F.

Data Breaches

If there is a Data Breach the relevant 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 relevant 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 Trust has responsibilities under the Data Protection Principles to keep data only for as long as needed.

In respect of the length of time that we should keep the data, we will follow the advice from the IRMS using their Records Management Toolkit for schools[2].

If paper is due to be destroyed it will be cross-cut shredded either by the relevant 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[3].

[2] http://irms.org.uk/page/SchoolsToolkit
[3] https://ico.org.uk/for-the-public/online/deleting-your-data/

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 Headteacher/Head of School or Chair of Governors.

Monitoring and Evaluation

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

Appendix A – Roles of Data Protection 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 Trust's data protection processes and advise 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 Trust about the 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 Trust'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 Trust 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, students 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 Trust if/when it should conduct an audit, which areas staff need training in, and what the DPO/DPL roles should involve.
- report to the Board of Directors on the Trust'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 Trust'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 Strategic Leadership Teams to ensure GDPR compliance;
- assist with any additional tasks necessary to keep the Trust 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 Trust;
- 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 Directors;
- providing telephone and email advice and support;
- providing regional training for the DPL and other staff;
- providing school based on-demand training.

Appendix B – Data Protection Lead Role

Data Protection Lead Responsibilities

To:

- verify that the Trust 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 Trust'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, students 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 Strategic Leadership team 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 Trust;
- 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 – Data Asset Audit

Each 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.

Data Asset Audit Document (Example)

Description of service	Type of data	Reason to hold data	Where is data stored?	Is the data shared with anyone?	Risks
SIMs Data	Personal and Sensitive Data	Statutory Duties Education Act	Server	DfE LA MAT	Lost passwords Inappropriate viewing Printouts Exchange agreement with Somerset LA Careful positioning of monitors

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: Amy Brittan - dposchools@somerset.gov.uk

Data Protection Lead:

Date completed:

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/Head of School 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**.

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/Head of School 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 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 will be recorded.

The process that will be followed is listed below:

- inform the DPL in the school (and the Headteacher/Head of School if necessary);
- record the details of the breach, updating this record where necessary (see next page);
- 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.

Data Breach Record

Date: / /	Person responsible for dealing with breach				
Outline of breach					
Which data subjects are involved					
Data type involved					
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					
Actions taken					
Preventative action suggestions – including training					
Notes					
Actions approved by		Date	/ /		