Buckler's Mead Academy

Policy Document

DATA PROTECTION POLICY

Policy Title:	Data Protection Policy
Author:	IT Manager / Matt Powell
Document Reference:	SPOL/MAN0218/019
Date Produced:	15/06/2018
Recommended by (Advisory Group / Committee / SLT):	Management committee
Date Adopted:	July 2018
Date published on website (if applicable):	July 2018
Signed By:	 ……. Chair of Directors
Review Frequency:	Annually
Review Date:	Summer 2019
Please note: The version of this document contained within the 'Policy Documents' Folder on BMStaff (T:\Admin\Policies and Procedures) is the only version that is maintained.	

1. Introduction

Bucklers Mead Academy 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.

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

2. The Data Controller and the Designated Data Controllers

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

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 available on the ICO's website.

The Academy has identified its designated Data Processing 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, Deputy Headteacher, and the Business Manager.

3. Responsibilities of the Academy

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

a) register with the Information Commissioners Office (ICO);
b) keep and up to date Data Asset Audit (See Appendix C) which lists all known uses of personal data in the school;
c) verify that all systems that involve personal data or confidential information will be examined to see that they meet the Data Protection Act 2018 Regulations;
d) inform all users about their rights regarding data protection;
e) provide training to ensure that staff know their responsibilities;
f) monitor its data protection and information security processes on a regular basis, changing practices if necessary.

4. 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 who do not have the authority to view the data;
b) is kept securely in a locked filing cabinet or drawer when not being used;
c) is stored on a secure password protected local or network drive;
d) if kept on removable storage (laptop, tablet, USB memory stick) approved by the school, 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 to any unauthorised third party;

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

Staff should note that unauthorised disclosure or transgression of the above statements will investigated, and may result as a disciplinary matter.

5. Responsibilities of Parents / Guardians

The Academy will inform Parents/Guardians of the importance of the personal data the Academy uses and the importance of keeping this up to data. This process will include at least an annual data collection sheet (with the return of this document being recorded) and reminders in newsletters and at tutor or class meetings.

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.

6. The right to access information

All people having personal data stored by the Academy have the right to:

a) obtain from the Academy confirmation as to whether personal data concerning him or her are being processed;
b) 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 parties 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 Academy 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 are 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.

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

d) have a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Academy 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.

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

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

The Academy 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 (or their parental right) should make a request in writing and submit it to the Headteacher or the chair of Directors. The process for dealing with these requests is outlined in Appendix E.

Commented [Mf1]: Or Business Manager, or A.Another?

The Academy 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. They may be an administration charge which will be stated once the enquiry is made.

7. 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 Act 2018) 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.

8. Data breaches

If there is a Data Breach the Academy 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 risk to the individual the Academy 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 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/ and 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 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.

9. Data Retention Policy

The Academy has responsibilities under the Data Protection Principles to keep data only for as long as necessary.

In respect of the length of time that schools should keep the data the Academy will follow the advice from the IRMS using their Records Management Toolkit for schools. http://irms.org.uk/page/SchoolsToolkit

If paper is due to be destroyed it will be cross-cut shredded wither by the Academy 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 https://ico.org.uk/for-the-public/online/deleting-your-data/

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

10. 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.

11. Monitoring and Evaluation

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

12. Contacts

If you have any enquires in relation to this policy, please contact the Headteacher.

Further advice and information is available from the Information Commissioner's Office www.ico.gov.uk

Appendix A – Role of Data Protection Officer

According to Article 37(5), the Data Protection Officer (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.

Within the Academy 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 Academy's data protection practices on a day to day basis.

Data Protection Officer Responsibilities

To:

- advise the Academy about their obligations under the Data Protection Act 2018;
- support the DPL in developing a joint understanding of the Academy'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 Academy's policies are followed, through:
    - Assigning responsibilities to individuals;
    - Awareness-raising activities;
    - Cordoning staff training;
    - Conducting internal data protection audits;
- advise on and assist the Academy 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 focussing mostly on these
    - advising the Academy 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 Academy'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 Academy'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 Academy;
- 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 Academy;
- 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 Acacemy 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 Academy 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 Academy has registered with the ICO;
- support the DPO in advising the Academy about their obligations under the Data Protection Act 2018;
- support the DPO in developing an understanding of the Academy'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 Academy'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 Academy;
    - 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 Academy's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - coordinating 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 Academy;
- work with the Senior Leadership team at the school to ensure GDPR compliance;
- assist with any additional tasks necessary to keep the Academy 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 Academy;
- 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

The Academy 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
Moodle	Potential sensitive data e.g. grades and performanc e	Learning tool	In the cloud by MoodleAny where. Held in London and Bristol. Contract checked	Parents	Lost passwords Inappropria te viewing
ClassDojo	Name and behaviour information	Tool to assist with behaviour manageme nt	In the cloud by Class Dojo		Not in EEA? Display on whiteboard

A template of this document can be found:

https://slp.somerset.org.uk/sites/edtech/Data%20Protection/Data%20Protection/Data%20Protection%20Pack/eLIM%20-%20Data%20Asset%20Audit.docx

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 Leadership Team 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.

<table>
<tr><td colspan="4">Describe the service</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Describe the data collected and the possible uses of the data</td></tr>
<tr><td colspan="2" rowspan="2">List of data held</td><td colspan="2">Collection of data</td></tr>
<tr><td colspan="2">Possible uses</td></tr>
<tr><td colspan="4">Identify the privacy, related risks and possible solutions To be discussed with the Data Protection Lead</td></tr>
<tr><td>Privacy issue</td><td>Risk to individuals</td><td>DPA Risks</td><td>Possible Solutions</td></tr>
<tr><td>1.</td><td>•</td><td>•</td><td>•</td></tr>
<tr><td>2.</td><td>•</td><td>•</td><td>•</td></tr>
<tr><td>3.</td><td>•</td><td>•</td><td>•</td></tr>
</table>

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:

Date completed:

The template for this document can be found at:

https://slp.somerset.org.uk/sites/edtech/Data%20Protection/Data%20Protection/Data%20Protection%20Pack/PIA%20-%20Privacy%20Impact%20Assessments/eLIM%20-%20PIA%20blank.docx

Appendix E - Handling a Subject Access Request

Requests for information must be made in writing; which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

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 for example:

- Passport
- Driving licence
- Utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

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

Commented [Mf2]: Ensure that this complies with GDPR guidelines. Do we have the legal right to decide whether a child is competent or not?

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.

The Academy may make a charge for additional copies of information requested beyond the initial request, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records, schools can charge up to £10 to provide it.
- If the information requested is only the educational record, viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

Commented [Mf3]: Does this still apply?

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. The 40 day statutory timescale still applies.

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.

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

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.

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.

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.

Process on receiving a Subject Access Request

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

- inform the DPL in the Academy (and the Headteacher if necessary);
- 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;
- 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 (Freedom of Information) 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 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 Academy (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 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;
- 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				
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	/ /		

Appendix H - Complaints

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

Further advice and information can be obtained from the Information Commissioner's Office

School Privacy notice for student induction packs

What is your 'Personal Data'?

Personal data is information that says something about you as an individual, so it would normally include your name, and / or contact details, or even a photograph of you.

What kind of information do we hold about you?

Apart from information you give us, we may also receive information about you from your previous schools, the local authority and the Department of Education (DfE).

This information will include you and your parents / guardians contact details, your assessment results, attendance information, any exclusion information, where you go after you leave us and personal characteristics such as your ethnic group and any medical conditions, special educational or dietary needs you want us to know about.

If you are aged over 14, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.

Without your consent, we will not process any personal data about you which we do not need.

Why do we need your information?

We need to use your personal data in order to

- support your learning
- monitor and report your progress
- provide appropriate pastoral care
- provide services needed while at the school; and
- assess the quality of our service

The purpose of processing your information is to provide you with the best education we can, as well as to meet our other legal requirements.

The legal basis for using this personal data are various Acts of Parliament including the Education Act 2011, Children's Act 2004 and Equality Act 2010.

For certain 'special categories' of data (like health or ethnicity information) we rely on your consent. This means you will be asked by us if agree to us holding this information about you.

Privacy Notice (How we use student information)

The categories of student information that we process include:

- personal identifiers and contacts (such as name, unique student number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as key stage 1 and phonics results, post 16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- biometric finger print information (for the academy's cashless catering system)

This list is not exhaustive, to access the current list of categories of information we process please request to see our data asset register.

Why we collect and use student information

The personal data collected is essential in order for the school to fulfil their official functions and meet legal requirements.

We collect and use student information, for the following purposes:

a. to support student learning
b. to monitor and report on student attainment progress
c. to provide appropriate pastoral care
d. to assess the quality of our services
e. to keep children safe (food allergies, or emergency contact details)
f. to meet the statutory duties placed upon us for DfE data collections

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing student information are:

- for the purposes of (a), (b), (c) & (d) in accordance with the legal basis of Public task: collecting the data is necessary to perform tasks that schools are required to perform as part of their statutory function

- for the purposes of (e) in accordance with the legal basis of Vital interests: to keep children safe (food allergies, or medical conditions)

- for the purposes of (f) in accordance with the legal basis of Legal obligation: data collected for DfE census information

    - Section 537A of the Education Act 1996
    - the Education Act 1996 s29(3)
    - the Education (School Performance Information) (England) Regulations 2007
    - regulations 5 and 8 School Information (England) Regulations 2008
    - the Education (Student Registration) (England) (Amendment) Regulations 2013

In addition, concerning any special category data:

- conditions a, b, c and d of GDPR - Article 9

How we collect student information

We collect student information via registration forms at the start of each academic year. In addition, when a child joins that Academy from another school we are sent a secure file containing relevant information.

Student data is essential for the academy's operational use. Whilst the majority of student information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with GDPR we will inform you at the point of collection, whether you are required to provide certain student information to us or if you have a choice in this.

How we store student data

We hold student data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please contact the Business Manager.

Who we share student information with

We routinely share student information with:

- schools that the students attend after leaving us
- our local authority
- youth support services (students aged 13+)
- the Department for Education (DfE)

Why we regularly share student information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / student once they reach the age 16.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

- This enables them to provide services as follows:
- post-16 education and training providers
- youth support services
- careers advisers

Data is securely transferred to the youth support service via a secure file transferring system and is stored within local authority software.

For more information about services for young people, please visit our local authority website.

Department for Education

We are required to share information about our students with the Department for Education (DfE) either directly or via our local authority for the purpose of data collections, under:

- Section 537A of the Education Act 1996
- the Education Act 1996 s29(3)
- the Education (School Performance Information) (England) Regulations 2007
- regulations 5 and 8 School Information (England) Regulations 2008
- the Education (Student Registration) (England) (Amendment) Regulations 2013

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under GDPR, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Business Manager at the Academy.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:

- The Business Manager at the Academy
- Our local authority http://www.somerset.gov.uk/contact-us

How Government uses your data

The student data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Student Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Student Database (NPD)

Much of the data about students in England goes on to be held in the National Student Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-student-database-user-guide-and-supporting-information

Sharing by the Department

The law allows the Department to share students' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 students per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided student information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-sha

To contact DfE: https://www.gov.uk/contact-dfe

If you would like to discuss anything in this privacy notice, please contact: Ian Gover, School Development Officer, Somerset LA – dposchools@somerset.gov.uk