Data Protection Policy

Bridgwater & Taunton College Trust

Signature of Andy Berry **On behalf of sponsor**		Date 15/10/20
Signature of Peter Elliott **On behalf of Bridgwater College Trust**		13/10/20

Review by full Board of Trustees **Approval Date**	15th October 2020
Policy Renewal Date	September 2022

Contents

1. Aims 3
2. Legislation and guidance 3
3. Definitions 3
4. The Data Controller 4
5. Roles and responsibilities 4
5.4 All staff 5
5.5 Data Protection Measures 5
6. Data protection principles 6
7. Collecting personal data 6
8. Sharing personal data 7
9. Subject Access Requests (SAR) and other rights of individuals 8
10. Personal requests to see educational record 10
11. Biometric recognition systems 10
12. CCTV 11
13. Photographs and videos 11
14. Data protection by design and default 12
15. Data security and storage of records 12
16. Disposal of records 13
17. Personal data breaches 13
18. Training 14
19. Monitoring arrangements 14
20. Links with other policies 14
Appendix 1: SAR Breach Form 15
Appendix 2: REPORTING A DATA BREACH.....17

1. Aims

Bridgwater & Taunton College Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). The Trust is committed not only to legal compliance, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individual with whom it deals.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for Subject Access Requests (SAR).

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our Funding Agreement and Articles of Association.

3. Definitions

Personal data: Any information relating to an identified, or identifiable, individual. This may include the individual's name, identification number, location data, and online identifier such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data: Personal data which is more sensitive and so needs more protection, including information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (such as fingerprints, retina and iris patterns) where used for identification purposes, health (physical or mental) and sex life or sexual orientation.

Processing: Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject: The identified or identifiable individual whose personal data is held or processed.

Data Controller: A person or organisation that determines the purposes and the means of processing of personal data.

Data Processor: A person or other body, other than an employee of the data controller, who processes personal data on behalf of the Data Controller.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

Our Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. This policy does not form part of an employee's contract of employment and may be amended at any time.

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

Full details on the DPO's responsibilities are set out in the job description.

The Trust's DPO is contactable via btcdataprotection@educ.somerset.gov.uk

5.3 Headteacher/CEO

The Headteacher of a school or CEO for Central Services acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any charges to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have an concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach and is to be reported
    - Whenever they are engaging in a new activity that may affect the privacy rights of individual (DPIA to be completed)
    - If they need help with any contracts or sharing personal data with third parties

5.5 Data Protection Measures

All employees, agents, contractors, or other parties working on the Trust's behalf must comply with the following when working with personal data:

- When data is erased due to it no longer being needed, it must be securely deleted and disposed of. Hard copies should be shredded, and electronic copied should be deleted securely
- Personal data may only be transmitted over secure networks. Transmission over unsecured networks is not permitted in any circumstances
- Personal data may not be transmitted over a wireless network if there is a wired alternative available
- Personal data contained in the body of an email, sent or received, should be copied from the email and stored securely. The email should be deleted and temporary files should also be deleted
- Where personal data is sent by fax, the recipient should be informed in advance and waiting by the fax machine to receive the data
- Where personal data is transferred in hardcopy form it should be passed directly to the recipient
- No personal data may be shared informally or transferred to any employees, agents, contractors or other parties. If an employee, agent or sub-contractor, or other party working on behalf of the Trust requires access to any personal data that they do not have access to, such access should be formally requested from the CEO
- Personal data (hardcopy and electronic stored on removable media) should be stored securely in a locked box, drawer, cabinet or similar
- Personal data must be handled with care at all times and not left unattended or on view. If personal data is being viewed on a computer screen and the computer in

question is to be left unattended for any period of time, the user must lock the computer screen before leaving it

- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Trust or otherwise. In the event of any such approval, strictly in accordance with all instructions and limitations described at the time approval is given, and for no longer than is absolutely necessary
- No personal data should be transferred to any device personally belonging to an employee, and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Trust where the party has agreed to comply fully with this Policy
- All personal data stored electronically should be stored securely using passwords and data encryption. This store should be backed up, which should also be encrypted
- All passwords used to protect personal data should contain a combination of uppercase and lowercase letters, numbers and symbols, and should not be easily guessed
- Under no circumstances should passwords be written down or shared between employees, agents, contractors, or other parties working on behalf of the Trust. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords

6. Data protection principles

The GDPR is based on data protection principles that our Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specific, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processes
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**
- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering in a contact

- The data needs to be processed so that the Trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individuals e.g. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the **public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in GDPR and DPA 2018.

For pupils in primary school:

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventative services).

For pupils in secondary school:

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 and has a sufficient level of understanding to make this decision, which will be judged on a case-by-case basis (except for online counselling and preventative services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

If a data subject informs the Trust that personal data held by the Trust is inaccurate or incomplete, the data must be rectified, and the data subject must be informed of this rectification within one month of receipt of the notification.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with our Data Retention Policy.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention and detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as along as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests (SAR) and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period (according to our Data Retention Policy)
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request please complete the SAR Access request form (Appendix 1) they must immediately forward it to the DPO email btcdataprotection@educ.somerset.gov.uk

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implication of a subject access request, or have given their consent.

For primary school subject access requests:

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request (SAR). Therefore, most subject access requests from parents or carers of pupils at our Trust may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

For secondary school subject access requests:

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implication of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Trust may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a requests, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (SAR) (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive a subject access request please complete the SAR Access request form (Appendix 1) they must immediately forward it to the DPO email btcdataprotection@educ.somerset.gov.uk

10. Personal requests to see educational record

Parents/carers wishing to access their child's educational records should complete a Subject Access Request form and submit according to the section above. Depending on the age of your child, this will determine whether their consent will be needed. Please see above sections regarding primary and secondary school subject access request submissions.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system, (for example, pupils use finger prints to withdraw books from the library, or for school meals) we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child takes part in it. The Trust will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric systems. We will provide alternative means of accessing the relevant services for those pupils. For example offer PIN or name identification.

Parents/carers and pupils can object to participation in the school's biometric recognition systems, or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent/carer.

Where staff members or other adults use the school biometric systems, we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw their consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV and please refer to the Trust's CCTV Policy.

We do not need to ask individual's permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be made via the CCTV request form found within the CCTV Policy and sent to the DPO email btcdataprotection@educ.somerset.gov.uk

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our Trust.

For primary schools:

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communications, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

For secondary schools:

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communications, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our E-Safety Policy for more information on our use of photographs and videos.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents high risks to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly conducting reviews and audits to test out privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subject, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see our Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law, and we will obtain a certificate of destruction.

17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." The cause of which can be accidental, or deliberate. This definition means that a breach is about more than just the loss of personal data.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a Trust context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils
- Email concerning personal data sent to the wrong person
- Staff taking personal data home and it being lost
- Personal data not securely disposed of, thrown in bin and not shredded. In the case of electronic hard drive, being discarded before it has been wiped of personal data
- Memory stick containing personal data that has not been encrypted is lost

18. Training

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary and all staff will be expected to complete the in house data protection training course.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 2 years and shared with the full Board of Trustees.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of Information Publication Scheme
- Privacy Notice
- Employee Privacy Notice
- Candidate Privacy Notice
- E-Safety Policy
- Acceptable User Agreement for pupils and staff
- Data Retention Policy
- CCTV Policy

Appendix 1

DATA BREACH REPORTING FORM

This form should be used to report details of an actual or suspected breach.

Email this completed form to the Data Protection Officer btctrust.dataprotection@educ.somerset.gov.uk. Please retain a copy for your records.

Do not notify affected data subjects. The DPO will determine who should be notified and how.

There are strict time scales for reporting the initial incident to the DPO and subsequent notification to the ICO (Information Commissioner's Office). The ICO requires notification within 72 hours of the breach. Failure to comply can result in significant fines for the organisation.

Reported by		**Department/School**	
Contact telephone number		**Date of this report**	
Date of incident		**Date of discovery of actual or suspected breach**	
Summary of the facts (Provide as much information as possible, including the amount, sensitivity and type of data involved)			
Cause of the actual or suspected breach (Provide detailed account of what happened)			
Is there a breach of employee, pupil or customer confidentiality?			
Who is or could be affected by the actual or suspected breach? (Include number of data subjects)			
Impact (or potential risk) of the event on Data Subject			
Any remedial actions taken			

A personal data breach can include the loss, destruction, corruption, unauthorised access to, or alteration of personal data. This definition is more than just personal data being lost. This can include deliberate or accidental causes.

If in doubt that a breach has occurred, complete the form and return to the DPO who can assist and advise.

Appendix 2

REPORTING A DATA BREACH

WHAT IS DATA?

Data refers to Personal Data: any information relating to a person(s) allowing them to be identified & includes the loss, destruction, corruption, un-authorized access to, or alteration of personal data. It can include deliberate or accidental causes.

DATA BREACH OCCURS

You should report a data breach as soon as you become aware of it.

STEP 1. Complete a Data Breach Reporting form (Retain a copy for your records)

Do not notify data subjects of the breach. The DPO (Data Protection Officer) will determine who should be notified and how. But if you can stop the escalation ie asking someone to delete an email sent in error please do so asap.

STEP 2. Send the completed form to btctrust.dataprotection@educ.somerset.gov.uk

STEP 3. Data Breach form is received and recorded on the register.

STEP 4. If any remedial actions have been taken the DPO will follow this up with you.

A report will be made to the ICO by the DPO if necessary and any less formal action/training will be advised.