Bridge School Malvern

Data Protection Policy

This Data Protection Policy is divided into three sections and 2 appendices:

Section 1 – Privacy Notice (How we use pupil information)
Section 2 – Privacy Notice (How we use workforce information)
Section 3 – Data Flow
Appendix 1 – General Digital Data Safety & Security Procedures (Guidelines for all staff to follow).
Appendix 1 – Additional Digital Data Safety & Security Procedures (Additional Guidelines for Staff with IT repsonsibilities).

Section 1 – Privacy Notice (How we use pupil information)

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, date of birth and address)
- Characteristics (such as ethnicity, language, nationality, country of birth)
- Attendance information (such as sessions attended, number of absences and absence reasons and exclusions)
- EHCP and other referral records
- Welfare concerns
- Academic/vocational progress

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information for DfE census purposes (Education Act 1996) and for school to school transfer purposes.

Processing is necessary for the performance of a contract to provide education provision. (GDPR Article 6, 8 Feb 2018).

Processing is necessary for compliance with a legal obligation to provide census information and comply with safeguarding measures. (GDPR Article 6, 8 Feb 2018).

Collecting Pupil Information
Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data
We retain the following pupil information:

- Student Central Register, pupil personal information, academic progress, welfare concerns, behavioural incidents and reporting data – will be retained permanently in encrypted electronic files and secured with at least one 'secure password'
- Pupil personal files (hard copies) will be passed on to the school the child attends after leaving the Bridge or until the child is 25 years old and then shredded.

Who we share pupil information with
We routinely share pupil information with:

- schools that the pupil attends after leaving us
- the local authority
- the Department for Education (DfE)
- Educational psychologists

Why we share pupil information
We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

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.

School transfer of documents
These will take place in accordance with the Department for Education's S2S (School to School) facility and guidance.

Information security

The following standard procedures are in place:

- Offices containing personal data will be kept locked when left unattended.
- Manual records containing personal information will be locked away in a cabinet or drawer when not in use.
- When documents containing personal information have reached the end of their life dispose of them by shredding
- Personal information will not be given out over the telephone
- Digital Data will be secured according to the procedures set out in Appendix 1 General Digital Data Safety & Security Procedures and Appendix 2

Youth support services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil 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

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Pupils aged 16+

We will also share certain information about pupils 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

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

The National Pupil Database (NPDB)

The NPD is owned and managed by the Department for Education and contains information about pupils 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.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

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

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

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

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

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

Requesting access to your personal data

Under data protection legislation, parents and pupils 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 Kathleen Barclay.

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
- claim compensation for damages caused by a breach of the Data Protection regulations

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

Process for right of rectification and erase
Employees and parents/guardians both have the right to access their personal data. Please apply to Kathleen Barclay 01684 311632

Process to ensure data remains accurate and up to date
Applications will be made to parents/guardians for up to date data at the start of each academic year.

Contact
If you would like to discuss anything in this privacy notice, please contact: Sue Hornby or Kathleen Barclay, 01684 311632.

Section 2 – Privacy Notice
(How we use school workforce information)

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, address, next of kin)
- payroll information (bank details, national insurance number)
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)

NB: A record is kept of DBS checks, but DBS certificates are the property of the employee.

Criminal offences committed whilst an employee of the Bridge

Criminal offences that occur whilst an employee of the Bridge must be declared and the information will be held on their HR record. This will only be disclosed to future employers if it is deemed relevant to that employer.

NB: Employees that are found guilty of criminal offenses that pose a safeguarding risk will have their contracts terminated and the LEA officer designated to lead on child protection/local authority social services designated manager for child protection. will be informed. Criminal offenses that do not pose a safeguarding risk will be considered independently and advice will be sought from the board of governors.

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid

The lawful basis on which we process this information
We collect and use employee information for DfE census purposes (Education Act 1996).

Processing is necessary for the performance of contracts to provide education provision, and employment. (GDPR Article 6, 8 Feb 2018).

Processing is necessary for compliance with a legal obligation to provide census information and comply with safeguarding measures. (GDPR Article 6, 8 Feb 2018)

Collecting this information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information
We retain the following employee information:

- Staff Central Register – will be retained permanently (electronic database)
- Personal HR files (hard copies) will be securely destroyed when staff leave the employment of Bridge School Malvern/Bridge Business Centre.

Information security
The following standard procedures are in place

- Offices containing personal data will be kept locked when left unattended.
- Manual records containing personal information will be locked away in a cabinet or drawer when not in use.
- When documents containing personal information have reached the end of their life dispose of them by shredding
- Personal information will not be given out over the telephone
- Digital Data will be secured according to the procedures set out in Appendix 1 "General Digital Data Safety & Security Procedures" and Appendix 2 "Additional Digital Data Safety & Security Procedures".

Who we share this information with
We share, or may be required to share, this information with:

- company accountants (for payroll)
- the local authority
- the Department for Education (DfE)

Why we share school workforce information
We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Diane Hancock.

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
- claim compensation for damages caused by a breach of the Data Protection regulations

Process for right of rectification and erase
Employees and parents/guardians both have the right to access their personal data. Employees should apply to Diane Hancock 01684 311632

Process to ensure data remains accurate and up to date
Employees will have the opportunity to update data at their annual appraisal.

Process to securely dispose of personal data that is no longer required
Obsolete electronic data will be permanently deleted from hard drives.
Obsolete hard copy data will be shredded.

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

Process for data protection breaches
In the event of a data protection breach

- Immediate action will be taken to retrieve the data
- all relevant parties will be informed
- governors will be informed and a governor will be appointed to conduct an internal investigation
- the appointed governor will inform the IOC
- disciplinary action will be taken as necessary

Policy review
The Headteacher receives updates from DfE on data protection and will update this policy accordingly.

Further information
If you would like to discuss anything in this privacy notice, please contact Sue Hornby.

Section 3

Data flow – Pupils

WHAT DATA WE HOLD / SOURCE	PRIMARY DESTINATION	SECONDARY DESTINATION	USAGE	FORWARD DESTINATION
Sending Agency ● Personal Details ● Professional reports ● Referral details ● Relevant medical diagnosis ● SEN information ● Welfare concerns ● Behavioural incidents	● SENCO ● Assistant Head of Sixth Form	● DSL/Deputy DSL ● Deputy Heateacher (BSM) ● CEO (BBC) ● Pastoral Coordinator (BSM) ● Business Leads (BBC) ● Teaching & Learning Manager ● Coaching staff	● Central Student Register* (for census and planning) ● Individual Learning Plan* (to maximise pupil progress and experience; to ensure contract requirements are met) ● Personal Files (to provide good pastoral support)	● Future school ● Educational or health professional on request
Previous School - Education data - Exclusion record - SEN details				

NB: Incoming data is stored as supplied, either hard copy or electronically. Subsequent storage, movement and creation of data within the school is electronic.

Data flow – Staff

DATA STORED	STORAGE DESTINATION	AVAILABLE TO	FORWARD DESTINATION
• Names and previous names • Address • DOB • Next of Kin • Copy of driver's licence • Copy of passport • copy of qualification certificates • DBS • Criminal record • Convictions or warnings • CV • Reference • Appraisals • Disciplinary actions and warnings • Absence record	• HR folders (for security checks, safeguarding purposes and monitoring staff wellbeing). Both paper based and internal dbase (Hal) are used. • Staff Central Records (for census and planning) on internal dbase (Hal).	• Administrator with HR responsibility • Headteacher • Governor responsible for HR	• Future employer on request: • Dates employed from and to • Absence record • Disciplinary actions and warnings • Criminal convictions if relevant to future post

Data Protection Policy - Appendix 1

General Digital Data Safety & Security Procedures.

This appendix must be well understood by all staff. It contains details of general steps that need to be routinely kept by all staff. Staff are required to review they are adhering to these procedures at least once a year.

Rationale
Digital systems have become complex, we have more data in more places than ever before. Methods used by 'hackers' have become increasingly advanced, it is not reasonable for individuals to be fully aware of how this happens. Everyone needs to understand the steps they are required to take to keep data safe. Staff do not need to understand why we take these steps. If these procedures are unclear or believed to be erroneous then the IT Lead needs to be informed for possible revision.

One of the great advantages of digital data is the ease with which it can be shared. This is also a source of vulnerability. As well as safeguarding data against 'hackers' we need to safeguard against unsafe data sharing or leaving it printed matter in an inappropriate place.

Definitions
Digital Data - any information, files, pictures or other matter stored on computer, in cloud storage, phone, tablet or other digital device.

Sensitive Data - any data that contains the name or image of a student, alludes to a student or contains information about any individual or group of individuals who attend the Bridge School Malvern. This definition does not imply individuals or groups are explicitly defined - anonymous data can be 'sensitive'.

Data Security - keeping data safe from other people or organisations that have no right to the information.

Data Safety - keeping data safe from loss.

All Staff Responsibilities

1. Your security sensitive passwords are
   Your Laptop login
   Your Gmail login

2. These password must be secure, i.e.
    a. be at least 8 characters long
    b. use a mix of letters, numbers and special characters
    c. not use well know phrases, dates or names of people/pets
    d. have an element of randomness
    e. be unique - not used on any other account (whether associated with the Bridge or not).
    f. not be written down
    g. not be stored on your laptop
    (it can be stored in a 'secure' password manager e.g. Lastpass)
    h. not be known to anyone other than yourself (passwords for both Laptops and Gmail can be reset by our admin; your partner does not need to be your reminder).

3. All data and files which need to be kept safe or secure are to be kept on your 'bridge' GoogleDrive. This may be synced to a single folder on your school issued laptop (this is recommended for convenience).

4. No files are to be downloaded or synced onto any device that has not been explicitly approved by school management -

These devices are approved	**These devices are NOT approved**
School issued laptop	Your mobile phone
Any Chromebook enrolled onto our domain	personally owned computers

5. You should be aware that files kept outside a GoogleDrive sync folder on your laptop may not be recoverable in the event of laptop loss or breakdown.

6. You may use your personal mobile phone to access online data/emails from your Bridge GSuite if all these conditions are met
    a. Your phone cannot be 'brute force' accessed, i.e. it will lock after a small number of failed login attempts.
    b. If you use biometric login then face recognition security must be set high and no more than one finger is registered to unlock it.
    c. Your phone is never left unlocked unless you are using it (this includes in your pocket).

7. Personal computers may be used to access your school data but browsers must not store login in details, nor can data be downloaded or synced to personally owned computers unless explicitly agreed to.

8. All cloud services used as part of Bridge business must be within the Bridges domain (I.e. accessible only by an email ending in "@bridgeschoolmalvern.org").
9. When creating or signing into any online service for Bridge business the login email must be a Bridge domain email.
10. When sharing data use the most restrictive permissions possible without compromising the use of the information. In particular consider restricting forwarding, printing and downloading.
11. Use confidential mode when sending internal emails containing anything that might be considered sensitive data.
12. When sending emails with sensitive information outside the Bridge domain then they must be encrypted.

Signed by …… (Staff signature)

Date……

Data Protection Policy - Appendix 2

Additional Digital Data Safety & Security Procedures.

This appendix deals with matters of digital safety and security that pertain to system administrators and staff with specific IT responsibilities. Generally other staff do not need to be aware of these measures.

1. There are 4 levels or personal to ensure overall digital data security and safety.
    a. Internal **IT lead** - currently Richard Love
    b. **IT support** - currently Danielle Baxter and Emma Thomas
    c. An external **Security Insurer** - currently Jonathon Spaul
    d. An **external GSuite 'super admin user'** - Currently Garry Blott of RRA services.
2. The IT lead shall ensure the Security Insurer has access via a secure encrypted note all passwords to all parts of the Bridge IT systems and has an awareness of our systems and procedures.
3. The external GSuite 'super admin user' shall have full admin rights to our GSuite resources
4. The purpose of points 2 and 3 is to ensure the Bridge has a backstop guarantee that in the event of any concoinviencable change in internal staff the Bridge's systems are maintainable.
5. The only people with access to Admin rights on all staff issued laptops are the IT Lead, IT Support and external Security Insurer.
6. The IT Lead and IT support shall ensure all hard disks used to store potentially sensitive data are encrypted.
7. The IT Lead and IT Support shall support staff in understanding and keeping to the procedures set out in Appendix 1.
8. The IT Lead and IT Support shall conduct periodic audits of staff issued IT equipment.