Bridge School Malvern

Review period	Annually		
Document Owner			
Last reviewed	Dec 21	**Next review**	Dec 22

Data Security & Safety Policy (staff responsibilities)

This policy sets out the steps BSM takes to ensure BSM's digital data is maintained securely and safely. There are 3 parts to this policy

1. General Principles
2. Management of digital security and safety.
3. Staff Responsibilities -
   At least one part of this section is to be read, understood and signed by all staff, governors and anyone else given access to BSM online data during their induction.

Section 1 - General Principles

1.1 Rationale

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 printed matter in an inappropriate place.

The technical ramifications of data security and safety measures are complex. It is not the purpose of this policy to explain or justify the measures that are in place. This document seeks only to ensure staff understand what their responsibilities are and how to implement them.

The steps set out in this policy are designed to cover all foreseeable ways data can be lost. If these procedures are unclear or believed to be erroneous, then the IT Lead must be informed immediately.

1.2 Definitions

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

1.2.2 **Sensitive Data/Information** - any data or information in any form (including digital or printed) that contains the name or image of a pupil, alludes to a pupil or contains information about any individual or group of individuals (pupils, staff or volunteers) who attends the Bridge School Malvern (BSM). This definition does not imply individuals or groups are explicitly defined - anonymous data can be 'sensitive'.

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

1.2.4 **[Data] Safety** - keeping data safe from loss (i.e keeping it somewhere it can be retrieved in the event of electronic device failure). The term 'safety' in other contexts and other policies may have a different meaning.

1.2.5 **BSM Domain** - is any digital service owned by BSM (e.g. Hal), paid for by BSM or is accessed by a login which includes a web domain name owned by BSM (e.g. "bridgeschoolmalvern.org"). This includes all Google provided services including Gmail, Google Drive, Classrooms, Calendar etc. It also includes any service you log into using a BSM email. All digital services used as part of staff roles at BSM must be signed into using a Bridge Domain Email and will therefore also be part of the BSM Domain.

1.2.6 **Secure Password -** to be secure a password must meet the following criteria

a. Be of sufficient length (min 8 characters if truly random characters)
b. Be unique, must not be used for any other online access
c. Not use well known phrases, names of pets/kids/spouses/partners etc, dates or other things associated with you.
d. Have an element of randomness. The use of 3 three random words is highly recommended (see this article https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words)
e. Know only to you
f. Not stored anywhere in any form other than in a trusted secure online password manager (e,g, LastPass, Bitwarden, Dashlane etc.)

1.2.7 In this policy, the term 'staff' refers to paid employees, volunteers and governors.

1.3 Management responsibility to monitor and act

1.3.1 All systems and networks run by BSM may be monitored by management or by contractors. This monitoring may take place in a number of ways including (but not limited to)

a. Filtering and Monitoring systems
b. Google Workspace Admin
c. Examination of school owned devices
d. Network management tools (e.g. WiFi Cloud Controller)
e. Observation of usage by any other means

1.3.2 The purpose of this monitoring is

a. To identify potential weaknesses in our systems and inform changes in practice.
b. Investigate or highlight potential breaches of policy.
c. Inform changes to this and other relevant policies.

1.3.3 In the event of a potential breach of policy, or breach of security being suspected, the following action will be taken

a. Any user believed to be breaching policy or otherwise being suspected of being involved with a security breach then those users will have their accounts suspended pending investigation. Such action will be taken as a precautionary measure and not part of a disciplinary action.
b. SLT will be notified.
c. SLT in conjunction with the appropriate managers will agree a plan to rectify the problem.
d. Users whose accounts have been suspended will be reinstated only when it is believed such action does not pose a threat.
e. In the event a member of staff has not followed this policy, or that a data breach has occured due to any action a member of staff should reasonably know is risky then the SLT will take action in accordance with the Staff Disciplinary Procedure.

1.3.4 In the event that any monitoring or action taken results in new guidance or changes to policy management will inform staff as soon as practically possible.

1.4 Sharing data - principles

It is often necessary to share information with other people both inside and outside the school. The manner in which we do this is dependent on a number of factors including

- The technology used by the data/information receiver.
- Their IT awareness and competence.
- The level at which we can trust them to handle information safely (not just their intent but also their ability to understand how to handle sensitive information)
- The nature of the material

These factors are especially difficult to gauge when sharing information externally, especially with parents. Given the range of possibilities a prescriptive policy to cover all eventualities is not practical. To mitigate the risks, BSM staff and managers will only share information using the principles set out below.

1.4.1 Share only with those people who need it. The use of group email lists should be avoided unless everyone on that list needs the information.

1.4.2 Share only what the receiver needs, where necessary material shared may be a redacted version of the original.

1.4.3 Unless required, shared material should be as anonymous as possible without devaluing the material for its intended purpose.

1.4.4 Matter is shared using the most restrictive method compatible with the purpose of sharing, in particular

a. Keep all data within the BSM domain by sharing (rather than attaching or otherwise sending copies to the receiver).

b. The default practice is to restrict the receiver's rights to "copy, print or download" material. These actions should only be allowed if the receiver has an absolute need to take the data out of our domain and they have sufficient competence to understand their responsibilities.

c. If the receiver only needs to read a document, allow them "viewer" only permissions; only granting editing permissions if the receiver needs it (Editors have the ability to copy, print and download).

d. If the matter is being shared with more than one person/organisation consider different permissions for each according to their requirements, in line with the principle above.

e. In the event that data is shared outside our domain then it is the responsibility of the sender to ensure the receiver is fully aware of their responsibilities to keep the material secure, are competent to do so and are sufficiently trustworthy.

f. Any doubts about any matter concerning sharing are discussed with a manager with IT responsibility and/or SLT.

1.5 Responsibilities

1.5.1 **SLT** - have overall responsibility for all matters in this policy. However they expect delegated managers with IT responsibility to advise and inform them appropriately. SLT will ensure compliance with relevant law.

1.5.2 **Managers with IT Responsibility** - have responsibility for maintaining this and other relevant policies, ensuring they are up to date with current best practice and reflect what BSM has learnt from its own experience. They will advise the SLT on all data security matters including suitable purchases to be made and practices to be adopted or changed. They will liaise with external providers and maintain current expertise on data security issues.

1.5.3 **Other managers** - will be models of good practice. They will ensure that they, and the staff they supervise or otherwise work with, are well informed and supported in using good practice. They will report any concerns they have to SLT.

1.5.4 **All Staff** - will read this policy and ensure they understand all those parts of it that affect their practice. They will report concerns about policy, compliance, inconsistencies and any other concerns pertaining to data security to SLT or suitable manager. They will adhere to this and other relevant policies, including being aware of the information included within the Information Asset Register.

1.6 Related policies

Staff code of conduct

Disciplinary Procedure Staff and Volunteers

GDPR Policy

Information Asset Register

Section 2
Management of digital security and safety

This section deals with matters of digital safety and security that pertain to system administrators and staff with specific IT responsibilities. IT systems change rapidly, these measures are intended to be flexible enough to accommodate such changes, in the event that is not the case SLT will act under the best available advice to take appropriate measures.

2.1 There are several levels of personnel to ensure overall digital data security and safety.

a. **IT lead** - will advise SLT on all matters regarding Data Security and Safety, monitor the systems and periodically review the processes in place. They will additionally provide SLT with all information required to ensure continuation of IT systems in the event of any change is personal at BSM. Currently (September 2022) the IT Lead is Richard Love

b. **IT support** - staff with particular expertise and/or IT responsibility points. The roles of such staff will be set out in their job description.

c. **External support** - individuals or organisations with a contractual agreement with BSM to help manage Google admin or other data assets. At least one external individual or organisation is required to have full Google Super Admin User rights. Such agreements will require SLT approval. Currently (September 2022) this is just ict4.

2.2 At least one external support shall have full admin rights to our Google Workspace admin, they have those rights for two purposes

a. Assist the maintenance and ensure the smooth running of services they provide and BSM's Google Workspace services. In this capacity they are not authorised to access the content of individual user accounts.

b. In the event of BSM requiring access directly to a user's account, suspending an account or investigating the activity of a user, the External Support can be instructed by the SLT or Governors to carry out the necessary technical tasks.

2.3 The purpose of the points above are to ensure BSM has a backstop guarantee that in the event of any staff changes, the school's systems are maintained and that in the event of any staff member (including SLT and those with IT responsibilities) requiring investigation, the SLT and/or the Governors have the ability to act.

2.4 Access rights to Admin areas shall be agreed by the IT Lead in conjunction with the SLT.

2.5 The IT Lead shall carry out routine audits of equipment and staff practices to ensure there is good compliance with this policy and there is a culture of general good practice.

2.6 The IT Lead will support staff in understanding and keeping to the procedures set out in this policy.

2.7 The IT Lead will provide mandatory training for all staff each year, the training will include

   a. An update on changes to the policies or practice.

   b. Overview of the risks and concerns that have emerged since the last update.

   c. An assessment of staff comprehension of the policy and current good practice. Staff will be required to achieve a 'pass' in such an assessment to be able to continue accessing BSM online resources.

Section 3

The last part of this policy below must be signed by all staff, Governors or volunteers who use any part of BSMs digital assets.

There are four versions of this section, at least one part must be read and signed by every user of BSMs Google Workspace.

Section 3.1 Is for staff issued with a BSM Chromebook.

Section 3.1.a Is for staff issued who also access BSM online resources via a personally owned mobile phone.

Section 3.2 Is for users who access BSM Google Workspace via their own device.

Section 3.3 Is additional guidance for staff with a BSM issued Windows device in addition to a BSM issued chromebook.

SECTION 3.1

Staff Responsibilities for users with BSM Chromebook

Applicable to all staff with a school issued Chromebook.

In signing this document you are acknowledging that you understand the steps you are required to take and that you agree to follow them and that you will seek clarification on any points you don't understand.

Core responsibilities and rules

3.1.1 Only ever use a school issued Chromebook to access your Gmail, Google Drive, Hal or any other BSM online resource (there is an exception allowing use of personal mobile phones as long as your complete section 3.1.a)

3.1.2 Never allow any other person (including family, other staff or pupils) use any device signed in as you - including a BSM issued Chromebook.

3.1.3 Keep your Gmail and Hal passwords secure (see 1.2.6 in this policy) , unique and known only to yourself.

3.1.4 Only use online resources agreed by SLT or a Manager with IT responsibilities. All such services used in school must use a BSM email to sign it, use of accounts signed in using other emails are forbidden.

3.1.5 Never leave a device signed in as you unattended without putting it to a locked screen. Unattended includes you being in the same room but not completely aware of the device and who is near it. You should be the closest person to it at all times. Where that isn't possible we do have several safe logins staff can use where less attention is required (e.g. meetings@bridgeschoolmalvern.org).

3.1.6 If breaching any of the guidance in any way hinders your work, or you are not sure if an action is against the policy then don't do it. Speak to a Manager with IT responsibilities first to see if there is a way round it. Whatever you would have been stopped from doing is a small consequence in comparison to possible outcomes of a data breach.

Optional use of personal mobile phone to access work Google resources

3.1.7 Staff may use their personal mobile phone to access some BSM online resources (in particular GMail, Calendar etc.). Doing so is a personal choice and there is no compulsion or encouragement for staff to do so, however if you choose to use your mobile device you will need to complete section 3.1.a of this policy.

Use of other devices

3.1.8 The use of any other device to access any BSM online resource (including BSM Gmail, Google Drive, Calendar etc… and Hal) is forbidden unless explicitly agreed in writing by the SLT and a separate agreement has been signed.

Other provisions/guidance

3.1.9 When sharing data use the most restrictive permissions possible without compromising the use of the information. If a document contains any level of data sensitivity then normal practice would be to block 'options to download, print, and *copy'. It is always safer to 'share' information by file sharing rather than attaching or otherwise sending a copy of files.*

3.1.10 When sending sensitive content in the body of an email use confidential mode.

3.1.11 Further guidance on sharing data is explained in detail in section 1.4 of the Data Security Policy. If sharing outside BSM, staff need to be aware of that guidance and how to follow it.

3.1.12 Staff are not permitted to alter any settings on BSM equipment that could conceivably affect Data Safety or Security.

3.1.13 If you believe there is a potential security vulnerability it is your responsibility to report it to either SLT or a manager with IT responsibility.

<u>Declaration</u>

I have read Section 3.1 - All Staff Responsibilities. and I understand the professional responsibilities it describes and agree to abide by them. Breaches to these provisions will be gross misconduct and will be managed in accordance with the Staff Code of Conduct and other relevant policies including Disciplinary Procedure Staff and Volunteers,

Signed by …………………………………………… (Staff signature) Date……………

This section must be signed by all staff at their induction. Additionally all staff must undergo and pass mandatory training annually.

If these procedures are unclear or believed to be erroneous then the IT Lead must be informed immediately.

The terms "Sensitive [Data]" , "[Data] Security" , " [Data] Safety" and "BSM Domain" have the meanings as defined at the start of the Data Security Policy.

SECTION 3.1.a

Staff Responsibilities for users who choose to use their personal mobile phone to access BSM online resources

Rationale

Your phone is your own personal device and how you choose to use it is up to you. However if you wish to use it to access BSM online information then such information is the property of BSM and we are fully entitled to enforce our standards to ensure our data is safe. If these standards are not compatible with how you wish to use your phone then you cannot use your phone to access your BSM Google account for any purpose.

If you decide to use your personal mobile phone to access your BSM Google Workspace (including, Gmail, Drive, Calendar, Docs etc) all the conditions over the page must be met:

Conditions for using a mobile phone to access BSM Googleworkspace

3.1.a.1 Your phone is using an operating system still receiving security support .

3.1.a.2 Access to your BSM Google account is only via Google apps (not browser login or another email client)

3.1.a.3 If you use biometric login, face recognition security must be set to the highest setting and no more than one finger/thumbprint is registered to unlock it.

3.1.a.4 Your phone is never left unlocked unless you are using it (this includes in your pocket or by using 'Smart Lock' / 'Trusted Places' type features).

3.1.a.5 You are the only person who has access to your phone.

3.1.a.6 You phone does not sync gmail login (or other BSM logins) to any other device (this is of particular concern with Apple devices, if you use an iPad or iMac you may need to check they do not have access to your BSM Gmail via iCloud syncing)

3.1.a.7 You only use the device to access online resources, files are not downloaded to your phone.

3.1.a.8 The phone automatically returns to a lock screen within 5 seconds of in activity.

3.1.a.9 Your phone is never connected to insecure public WiFi networks (those not requiring a password).

3.1.a.10 You generally follow the guidance advised by the National Cyber Security Centre (e.g. https://www.ncsc.gov.uk/guidance/securing-your-devices)

Please fill in the following information

Your name …………………………………………………………………………………..

Make and model of phone ………………………………………………………………………..

Operating system version …………………………………………………………………………

Declaration

I have read and understood the above and will notify the IT Lead if I change my phone.

Signed by …………………………………………………… (Staff signature) Date…………

SECTION 3.2:

Users accessing BSM Google Workspace with their own personal device

This section sets out the precautions that must be taken by people with access to BSM sensitive digital data on devices not maintained by BSM (including school governors).

If there are any aspects of these procedures you are not clear about implementing it is your responsibility to seek support.

If these procedures are unclear or believed to be erroneous then the IT Lead must be informed immediately. The terms "Sensitive [Data]" , "[Data] Security" , " [Data] Safety" and "BSM Domain" have the meanings as defined in 'Data Security & Safety Policy (staff responsibilities) Section 1.2'

Rationale
BSM now has available online a vast amount of information, some of which is sensitive. This availability of information is having a positive impact on the operation of school. In general this information is well protected by a fully managed system which most users access via fully managed school issued devices providing a very secure gateway. This section provides precise guidance to those users, with access to sensitive data on devices that are not only unmanaged by the school but also not purchased or commissioned by BSM.

Key principles

- Google workspace provides a safe and secure set of cloud based tools for storing and managing data.
- Cloud based systems provide the safest and most secure environment to store digital data.
- When data is shifted from the cloud to either local drive storage or printed paper the security of that data is compromised.
- Printed data in particular poses the most likely potential breach of security of sensitive information and should be avoided in principle wherever possible.
- The security of a system can never be stronger than its weakest link.
- Small low risk vulnerabilities multiply if that vulnerability is repeated across many users.
- Data within the BSM domain is to some level within our control and is traceable while still in our domain, once it is downloaded, printed or shared outside the domain we lose all control and traceability of that information.

Steps required to maintain data security

3.2.1 Your google login is the gateway to the data shared with you, that password must be secure, i.e.

a. not use well know phrases, dates or names of people/pets
b. have an element of randomness
c. be unique - not used on any other account (whether associated with the Bridge or not).
d. not be written down
e. not be stored on any device
(it can be stored in a 'secure' password manager e.g. Lastpass, Bitwarden)
f. not be known to anyone other than yourself
(passwords can be easily reset by IT support or Richard at BSM).

Advice on generating strong passwords can be found on this link https://www.ncsc.gov.uk/news/ncsc-lifts-lid-on-three-random-words-password-logic

3.2.2 All data and files which need to be kept safe and secure are to be kept on your BSM domain Google Drive.

3.2.3 Your access to BSM domain resources is only made on devices personally owned by you and that reasonable steps are taken to ensure the device is secure, in particular

a. Internet access is via a secure connection
b. The device uses an up to date operating system that is still maintained by the supplier (Typically Windows 10 or higher).
c. The operating system is regularly updated with the supplier's security updates.
d. Reasonable steps are taken to ensure the device is protected against malware (e.g. WIndows users enable all advised security settings or use a maintained and updated third party system with a reputation at least as good as the default Windows system).
e. The browser does not store the login credentials to your BSM Google Workspace.

3.2.4 Files cannot be downloaded or synced onto any device other than one fully managed by BSM (or has been specifically set up by BSM in which case additional security measures will need to be agreed). In practice this means Google Drive and its contents can only be viewed via a browser.

3.2.5 All online services used as part of BSM business must be within the Bridge's domain (i.e. accessible only by an email ending in "@bridgeschoolmalvern.org").

3.2.6 When creating or signing into any online service for BSM business the login email must be a BSM domain email.

3.2.7 When sharing data use the most restrictive permissions possible without compromising the use of the information. If a document contains any level of data sensitivity then normal practice would be to block 'options to download, print, and copy'. If a document is shared allowing those options it can only be done so with the explicit agreement of a member of school management

3.2.8 Use confidential mode when sending internal emails containing anything that might be considered sensitive data.

3.2.9 Sensitive information can only be shared with parties outside the BSM domain if the receiver is known to have rigorous measures in place to maintain the security of the information.

I have read Section 3.2 and I understand the professional responsibilities it describes and agree to abide by them.

Signed by ……………………………………………… (Users signature)

Date…………………………………………

SECTION 3.3: Additional responsibilities for staff using Windows based devices in addition to a staff issued Chromebook.

This section must be signed in conjunction with section 3.1. This is a supplement to 3.1 in signing this it is presumed the staff member is accepting the responsibilities in Section 3.1 in addition to these

3.3.1 I acknowledge the Windows based device is not fully managed by BSM and is inherently less secure than the BSM issued Chromebook

3.3.2 The Windows device is only issued because there is an aspect to my work that cannot be easily done on a Chromebook

3.3.3 Wherever possible I will use the issued Chromebook in preference to the Windows device.

3.3.4 The Windows device will not be used for the following

a. Send, recieve or read emails from any BSM Gmail account
b. As a destination for downloading any files that could in any way be described as 'sensitive' as defined in this policy.
c. Access my GDrive by any means other than via a Chrome browser, and only then if absolutely necessary for the specific tasks I have been allocated the device for.
d. Syncing files from GDrive onto the local hard disk - files required on the Windows device must be downloaded individually and not contain any material deemed 'sensitive' as defined in this policy.
e. On occasion that a file needs to be downloaded to be usable (e.g. opening a password protect Word/Excel file) then once finished with the file is returned to safe cloud storage and 'secure deleted' from the Windows device.

3.3.5 Browsers will be set so they do not store login details for any account associated with BSM.

3.3.6 Device settings that could conceivably affect the security of the device or browsers must not be changed unless the change is agreed to in writing by a manager with IT responsibilities.

Advice must be sought on any aspect of this agreement that is not clear.

In exceptional circumstances some of the above may be waived but such agreements will be in writing and may require additional precautions which will be included in the waiver.

Breaches to these provisions will be gross misconduct and will be managed in accordance with the Staff Code of Conduct and other relevant policies

Signed by ……………………………………………… (Staff signature)

Date………………………………