The Blue Coat School

INFORMATION SECURITY POLICY

Approved by the Governors' Safeguarding, Health and Safety Committee

Signed: ______________________________

(K Gilmore – Chair of Safeguarding, Health and Safety Committee)

Date: _____________________

Date of Next Review: Trinity 2026

This Information Security Policy was devised by the Bursar, The Estates & Compliance Manager and the Network Administrator, in consultation with the Headmaster and the Director of Marketing & Admissions.

The Blue Coat School Birmingham Limited

INFORMATION SECURITY POLICY

1. INTRODUCTION

1.1
Information security is about what Staff and the School should be doing to make sure that Personal Data is kept safe.

1.2
This Policy should be read in conjunction with the Employment Manual and other related policies including: Data Protection Policy; ICT Acceptable Use Policy; Online Safety; Privacy Notice for Staff; Privacy Notice for Pupils and Parents; Information and Records Retention Policy; Staff Code of Conduct; Safeguarding and Child Protection Policy, Remote Learning Policy and Guidance for Staff on the Use of Photographs and Videos of Pupils by the School.

1.3
This Policy applies to all staff (which includes Governors, agency staff, contractors, work experience students and volunteers) when handling Personal Data. This Policy may be changed at any time and, where appropriate, staff will be informed of any such changes by email.

2. SECURITY BREACHES

2.1
Information security breaches can happen in a number of different ways. All security incidents, breaches and weaknesses must be reported to the Bursar as soon as practicably possible. Possible security breaches include:

- accidently sending an email to the wrong recipient;
- mislaid papers which contain personal data; or
- loss or theft of any device used to access or store personal data (such as a laptop or a smartphone) or a suspicion that the security of any such device has been compromised.

2.2
In certain situations, the School must report an information security breach to the Information Commissioner's Office (the data protection regulator) and let those whose information has been compromised know within strict timescales. This would normally be reported by the Bursar who is the School Data Protection Officer.

2.3
Any breach of this Policy will be taken seriously and may result in disciplinary action. A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal. This Policy does not form part of any employee's contract of employment.

3. CRITICAL SCHOOL PERSONAL DATA

3.1
Data protection is about protecting information about individuals. However, some personal information is so sensitive that it is password protected and only accessible by key personnel as defined by their job role. This is called **Critical School Personal Data** and it includes:

- information concerning child protection matters;

- information about serious or confidential medical conditions and information about special educational needs;
- information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);
- financial information (for example about parents and staff);
- physical or mental health or condition;
- information relating to actual or alleged criminal activity.

4. GUIDANCE AND APPS

4.1

More detailed advice about Information Security is set out in Appendix 1. The applications used by the school, their purpose, the specific associated security arrangements and relevant notes are listed in Appendix 3.

5. PAYMENT CARD SECURITY POLICY AND PROCEDURES

5.1

The requirements for Payment Card Security are set out in Appendix 2.

6. MONITORING AND POLICY REVIEW

6.1

The Policy will be reviewed at least annually to ensure that it complies with statutory requirements and to ensure that any changes in practices are accurately reflected. It should be read in conjunction with the other policies as specified in 1.2 above. It will be presented to the Governors' Safeguarding and Health and Safety Committee for approval in the Trinity Term. The minutes of this meeting will be presented to the Governors.

APPENDIX 1 DATA GUIDANCE

1. USE OF COMPUTERS AND IT

1.1

A lot of data protection breaches happen as a result of basic mistakes being made when using the School's IT system.

1.2 Locking Computer Screens

Computer screens should be locked when not in use, even when only away from the computer for a short period of time. Computer screens can be locked by pressing the "Windows" key followed by the "L" key. Apple Mac machines can be locked by simultaneously pressing the following keys: Control + Command + Q. iPads can be locked using the lock button and they are defaulted to lock after 1 minute. Computers for use by teaching staff are configured to automatically lock if not used for 30 minutes and computers used by support staff will lock if not used for 5 minutes.

1.3 Use of the School's IT systems

1.3.1

Staff should ensure that they are familiar with any software or hardware used and in particular, what the software is supposed to be used for and any risks. For example:

- when using a "virtual classroom" which allows the upload of lesson plans and mock exam papers for pupils, then care must be taken to ensure that anything more confidential is not accidently uploaded;
- ensuring the proper use of any security features contained in School software such as software which allows the redaction of documents (i.e. "black out" text which cannot be read by the recipient). This must be used correctly so that the recipient of the document cannot "undo" the redactions; and
- taking extra care when storing information containing Critical School Personal Data.

1.4 Use of hardware and software not provided by the School

Staff must not use, download or install any software, app, programme, or service without permission from the Network Administrator. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to the School IT systems without permission.

1.5 Private cloud storage

Private cloud storage or file sharing accounts must not be used to store or share School documents.

1.6 Portable media devices

The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed unless those devices have been given to a member of staff by the School and training on how to use those devices securely has been received. The IT Department will protect any portable media device given to staff with encryption.

1.7 Disposal of School IT equipment

School IT equipment including laptops, iPads, printers, phones, and DVD must always be returned to the IT Department even if it is thought to be broken and no longer working.

2. PASSWORDS

2.1

Passwords must be strong and difficult to guess. Staff are encouraged to use passphrases derived from memorable sentences, such as song lyrics or personal phrases, combined with numbers or elements known only to the individual. Passwords must **not** include easily discoverable information, such as names, addresses, or dates of birth. Avoid creating passwords that are overly complex or difficult to remember, as this may lead to them being written down, which poses a security risk. Passwords must remain confidential and must not be shared with others or recorded in any written or digital format that could be accessed by others. There is an automatic 90-day expiry for passwords at which point staff are required to change their passwords.

2.2

Staff must not use a password which is used for another account. Staff must not use passwords used for private email addresses or online services for any school account.

2.3

Passwords (and any other security credential issued to staff such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else.

3. EMAILS

3.1

When sending emails staff must take care to make sure that the recipients are correct.

3.2 Emails to multiple recipients

3.2.1

School emails are sent HTTPS via Google Mail. If sent via the School Management System, this is also achieved via SSL > HTTPS.

3.3

If the email contains Critical School Personal Data then staff must take extra care to check the recipient(s) email before pressing send. The email system also includes a 'Confidential Mode'. If this is enabled, then the recipient cannot forward or print thus reducing the risk of misuse of emails. In addition to password protection, it is also possible to set an 'Expire' on an email so that it automatically deletes itself.

3.4 Encryption

Internal and external emails which contain Critical School Personal Data must be encrypted. For example, encryption should be used when sending details of a safeguarding incident to social services. To use encryption then staff need to always use Google Mail as supplied by the School. If it is necessary to provide the "password" or "key" to unlock an encrypted email or document then this should be provided via a different means such as a telephone call to the recipient to provide the password after emailing the encrypted documents.

3.5 Private email addresses

Private email addresses must not be used for School related work. Staff must only use their @thebluecoatschool.com address. This general rule also applies to Governors and The Friends. The Network Administrator will set up email accounts if required.

4. PAPER FILES

4.1 Personal Data files

Staff must ensure that papers which contain Personal Data are kept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.

4.2

Critical Personal Data is stored in cabinets which are located around the School as follows:

Cabinet	Access
Child protection records – located in the Main DSL's office	All DSLs have access.
Financial information – located in the Bursary.	All of the Finance Team have access.
Health information – located in the Health Centre.	School Matron and her Assistant have access.
Staff records – located in the Bursary.	The Bursar and Finance Manager have access.
Pupil records – located in the Pre-Prep Office and the School Safe.	Relevant admin personnel have access.

4.3 Disposal

Paper records containing Personal Data should be disposed of securely by shredding. Personal Data should never be placed in the general waste.

4.4 Printing

When printing documents, staff must ensure that everything is collected from the printer straight away, otherwise there is a risk that confidential information might be read or picked up by someone else. If staff see anything left by the printer which contains Personal Data then this must be handed to the Bursar. The School uses secure printing on all but a select number of printers which means that printing is only released when the sender attends the printer. However, printing sent from Apple Mac devices does not need to be released by the sender and extra care must be taken when sending items to the printer from an Apple Mac device. While the School takes technical steps to prevent a misprint or printing to the wrong location, staff should double check the printer location they intend to print to before proceeding. If the end user is unsure, they should seek assistance from the IT Department.

4.5 Filing

Staff should always keep a tidy desk and put papers away when the desk is left unattended. Paragraph 4.2 above states clearly where Critical School Personal Data should be kept.

4.6 Post

Staff also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post.

5. WORKING OFF SITE (e.g. SCHOOL TRIPS AND HOMEWORKING)

5.1

Staff might need to take Personal Data off the School site for various reasons, for example because they are working from home or supervising a School trip. This does not breach data protection law if the appropriate safeguards are in place to protect Personal Data.

5.2

For School trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it. Personal Data that is taken off site must be returned to the School.

5.3

Staff wishing to work from home should check with the Network Administrator regarding any additional arrangements required such as installing software on home computers or smartphones (see Section 6 below).

5.4

When working away from the School staff must only take the minimum amount of information with them. For example, a teacher organising a field trip might need to take information about pupils' medical conditions (for example, allergies and medication but this information must only relate to the pupils attending the trip).

5.5

Staff must not work on documents containing Personal Data whilst travelling if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see what is being done). If working on a laptop on a train, staff should ensure that no one else can see the laptop screen and no device should be left unattended where there is a risk that it might be taken.

5.6 Paper records

If it is necessary to take hard copy (i.e. paper) records then staff should make sure that they are kept secure. For example:

- Documents should be kept in a locked case. They should also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g. overnight).
- If travelling by train staff must keep the documents with them at all times and they should not store documents in luggage racks.
- If travelling by car, staff must keep the documents out of plain sight. Staff should be aware that possessions left on car seats are vulnerable to theft when the vehicle is stationary such as at traffic lights;
- If staff have a choice between leaving documents in a vehicle and taking them with them (e.g. to a meeting) then staff should usually take the documents with them and keep them on their person in a locked case. However, there may be specific circumstances when staff consider that it would be safer to leave them in a locked case in the vehicle out of plain sight. The risks of this situation should be reduced by only having the minimum amount of Personal Data with them.

5.7 Public Wi-Fi

When connecting to a public Wi-Fi staff must use HTTPS/SSL secured apps and websites. All of the services and apps the School uses are secured using this. Staff should check that the address bar at the top-left corner of the browser on the device being used says "HTTPS://".

5.8 Using School laptops, phones, cameras and other devices

Staff who require a laptop or other device as part of their role, or alternatively need to book out a School device, must seek permission from the Headmaster or Bursar and the IT Department will then confirm availability.

5.9

Critical School Personal Data should not be taken off the site in paper format save for specified situations where this is absolutely necessary, for example, where necessary for school trips (see above).

6. USING PERSONAL DEVICES FOR SCHOOL WORK

6.1 Using a personal Laptop or PC

6.1.1

If staff members use their own laptop or PC for School work then they must use the Cloud Services available through the School Intranet. Using this means that Personal Data is accessed through the School's own secure cloud network which is far more secure and significantly reduces the risk of a security breach. All links to these services are on the School website via the BCS Staff link. Staff must connect such devices to the BYOD network, which is firewall protected from the rest of the school network. *(See 6.2 below also.)*

6.2 Using a personal smartphone or handheld device

Staff should connect to the BYOD (Bring Your Own Device) Wi-Fi Network which helps to protect data integrity. This is password protected. The IT team will provide advice to staff members about connection if required.

6.3

Staff must not do anything which could prevent any software installed on their computer or device by the School from working properly. For example, staff must not try and uninstall the software, or save School related documents to an area of their device not protected, without permission from the Network Administrator first.

6.4

Appropriate security measures should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date.

6.5 Default passwords

If staff members use a personal device for school work which came with a default password then this password should be changed immediately. Please see section 2 above for guidance on choosing a strong password.

6.6 Sending or saving documents to personal devices

Documents containing Personal Data (including photographs and videos) should not normally be sent to or saved to personal devices, unless permission has been given by the Headmaster. This is because anything saved to personal computers, tablets or mobile phones will not be protected by the School's security systems. Furthermore, it is often very difficult to delete something which has been saved to a computer. For example, if a School document has been saved to a personal laptop because a member of staff wanted to work on it over the weekend, then the document would still be on their computer hard drive even if it was deleted it and the recycle bin was emptied.

6.7 Friends and family

Staff must take steps to ensure that others who use their device (for example, friends and family) cannot access anything school related on their device. For example, login details should not be shared with others and staff should log out of their account once they have finished working. Staff must also make sure that their devices are not configured in a way that would allow someone else access to School related documents and information. The IT Systems Administrator will provide advice should this be required.

6.8 When a member of staff stops using their device for School work

If members of staff stop using their devices for School work, for example:

- if they decide that they do not wish to use their device for School work; or
- if the School withdraws permission for them to use their device; or
- if they are about to leave the School then, all School documents (including School emails), and any software applications provided by the School for School purposes, will be removed from the device.

If this cannot be achieved remotely, staff members must submit the device to the IT Department for wiping and software removal. Staff must provide all necessary co-operation and assistance to the IT department in relation to this process.

APPENDIX 2   PAYMENT CARD SECURITY POLICY AND PROCEDURES

Adherence to this policy and the associated procedures is mandatory for all staff who handle or process card payments on behalf of The Blue Coat School

1. Where unavoidable staff may take payments using a Point of Sale terminal (PDQ machine). Payments should normally be taken on a "customer present" basis. When a successful payment is processed the paper "Merchant copy" receipt generated by the machine should be stored securely in a locked drawer / cabinet and the "customer copy" handed to the customer. Receipts should not be retained if there is no business need to do so.
2. If the transaction is declined, the customer should be informed immediately and asked to contact the card provider. Receipts should be handled in the same way as in Point 1
3. If the customer is not present, they may be asked to provide details over the phone. These must be entered directly by the staff member taking the call into the PDQ machine. Normally this should be done immediately while the customer is on the phone and card details should not be written down. Only if there is a genuine reason why the transaction cannot be processed immediately (e.g. loss of network) may details be written down. They must be stored securely in a locked drawer / cabinet, actioned as soon as possible and then shredded. The card- validation code or value (three digit or four-digit number printed on the front or back of payment card) used to verify card-not-present transactions must not be stored.
4. Confidential and sensitive information (e.g. card numbers) must never be sent unencrypted through end-user messaging technologies (such as e-mail, instant messaging, or chat). Card details should **never** be requested via e-mail. **On no account** should card details be processed if received this way. Emails must be deleted out of the inbox and deleted folder and a new message composed to the customer informing them that their card details will not be accepted via email.
5. Card details should **never** be requested via a paper booking/payment form.
6. All confidential and sensitive data will be retained only as long as required for legal, regulatory and business requirements and in a secured location (e.g. locked cabinet / safe).
7. Refunds can only be processed by a member of the Finance Team, and refunds are by Bank Transfer only and **not by the card machine.**
8. Supervisor cards must be stored in a securely locked drawer / cabinet out of sight and only used by a member of the Finance Team.
9. All Point of Sale terminals must be kept secure and not left unattended. They must be stored in a locked drawer / cabinet.
10. The Finance Manager will undertake a PCI-DSS (Payment Card Industry Data Security Standard) Compliance Review on an annual basis. This was last completed in January 2020.
11. Data Security Scans are conducted automatically by the IT Department using Panda Antivirus.

APPENDIX 3 SCHOOL APPLICATIONS

Application	What it can be used for	Specific security arrangements	Any other notes / comments
ISAMS	School MIS	Cloud HTTPS via SSL encryption. All staff have varying levels of access. All personal including children's sensitive data is kept here. Any changes to this database or access beyond "normal" means has to be given in writing by SLT. Access to this is suppled via an SSO process in conjunction with Google.	ISAMS will update the SQL database as they host it. They cannot make any changes to data without explicit consent from an authorising person at the school. All APIs associated with ISAMS are "read only" and have prior authorisation.
GroupCall	API middleman between iSAMS and Apple School Manager	Secure cloud-based API which transfers classroom data and structure from iSAMS to Apple School Manager to allow for granular iPad management for the pupils.	Managed by KSF & FAP.
Google Apps	Site wide collaboration	Cloud HTTPS supplied by Google. All staff and pupils have varying access to this. This stores the school's shared data and personal data. All the collaborative work and processes centre on this. Access to this must be given in writing from SLT.	Google host the majority of the school's shared data and will not change this. The management of this data is controlled by FAP & KSF.
Google Mail	School Email System	Cloud HTTP supplied by Google. All staff and pupils have varying access to this. Pupils have only "internal" access to this. Access to this has to be given in writing from SLT.	Google host the majority of the school's shared data and will not change this. The management of this data is controlled by FAP & KSF.
PaperCut	Photocopier Management	Cloud based printing, photocopying, and scanning for devices for staff across the school site	Supplied and supported by Konica Minolta. Managed in-house by FAP and KSF.
Furlong Maestro	Manage music lessons	Cloud based SSL/HTTPS with an API to our cloud-based MIS (iSAMS)	Support provided by Furlong School Data Systems. KSF manages the data internally with JEN.
Parents Evening System	Parents Evening Booking System	SSL API between itself (cloud based) and School MSI	A read only API exists between this and ISAMS. Managed by HRW & FAP.

Microsoft 365	Productivity	Saved to secure on premise or Cloud (Google Team Drive) location.	
Mail Chimp	Mailing subscription	Cloud based SSL/HTTPS	Managed by Marketing & Admissions Director
Adobe Creative Cloud	Cloud Productivity	On premise software connecting to cloud-based storage secured with SSL/HTTPS. Floating licenses for potentially any member of staff. Secured login enforced by Adobe and specific software must be downloaded.	Managed by FAP & KSF. Adobe may store saved data but will not change any of this.
Adobe Sign	Cloud Productivity	Completely web based electronic signatory software for use with signing various agreements and policies in school to replace paper records.	Managed by FAP and CG
Purple Mash	Cloud VLE	Cloud based secured with SSL/HTTPS. All staff members have write access to this, all pupils login and perform their set assignments.	Managed by FAP, KSF, NCH
Espresso	Cloud VLE	Cloud based secured with SSL/HTTPS. All staff members have write access to this, all pupils login and perform their set assignments.	Managed by FAP and KSF
Twinkl	Cloud VLE	Cloud based secured with SSL/HTTPS. All staff members have write access to this, all pupils login and perform their set assignments.	Managed by FAP, KSF & NCH.
Fuse Mail: VaultSMART	Cloud Email Spam & Archive	Cloud based secured with SSL/HTTPS. Interfaces with Google Mail via Mail Re-directing method. FAP & KSF have overall administrators access to this. Authorisation has to be given in writing by SLT to retrieve data from this.	Fuse Mail will scan all email coming in/out of the school. With the use of AI, a determination as to whether this is spam with a category will be allocated to each message. These also have read access to our mail to store within an archive.
Sage 50 Accounts – Cloud 50	Cloud based VM	A virtual Sage Accounts server in the cloud. Only FAP, BJC, QWM and KSF have access to this.	Supported and supplied by Cloud 50 solutions and managed in-house by FAP and KSF.

Sage 50 Business Cloud	Sage Cloud solution managed by external supplier.	This has been migrated in April 2023 to an external supplier, Cutter & Co Chartered Accountants.	Managed by BJC & GWM.
JAMF Pro	Cloud based Desktop & iPad/Mobile Device Management	Cloud based secured with SSL/HTTPS and direct APIs with Apple. Used for managing school device enrolled Apple Devices both desktop class and mobile/tablet Used by anyone on school site. Facilitates the iPad 1:1 programme.	Managed by FAP & KSF.
Google Device MDM	Cloud based Mobile Device Management	Cloud based secured with SSL/HTTPS and direct APIs with Google. Used for managing school device enrolled Android products such as the school issued phones. Assigned to specific users. List available on request.	Managed by FAP & KSF.
Panda Adaptive Defence 360	Cloud based antivirus software	Cloud based secured with SSL/HTTPS and direct APIs with Panda. Runs on Windows and Mac Workstations. All users affected. Protects against online threats.	Managed by FAP & KSF.
WCBS School Alumni	Cloud based Alumni MIS	Cloud based secured with SSL/HTTPS and direct APIs with Panda. Runs on Windows and Mac Workstations. All users affected. Protects against online threats. Only Dir of Ext Rel has full access to this database. Other nominated administrators have restricted access to this database.	WCBS Software support and maintain this database which is hosted in London. Managed by Marketing & Admissions Director.