EAST BARNET SCHOOL

"I want to learn"

INFORMATION SECURITY POLICY (Incorporating Data Protection)

Version 2.1

Review by Resources Committee:	25 May 2021
Adopted by Governing Body:	07 June 2021
Next Full Review Due:	Summer 2024
Reviewer:	H. Chamberlain
Governor Link:	Data Link Governor or Chair of Resources

INFORMATION SECURITY POLICY

East Barnet School, Chestnut Grove, East Barnet, Herts EN4 8PU

1. Statement of Principle

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data. The School is committed to ensuring the security of all information that it holds and will implement the highest standards of information security.

1.1. This document sets out the measures in place to:

- protect against potential breaches of confidentiality
- ensure that all information assets and IT facilities are protected against damage, loss or misuse
- support our *Data Protection Policy* in ensuring all staff are aware of and comply with both UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the School of the requirements for information security and the responsibility placed on all staff to protect the confidentiality and integrity of the information that they personally handle.

2. Introduction

2.1. Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

2.2. Staff are referred to the School's *Data Protection Policy* and *Data Breach Policy* for further information. These policies are also designed to protect personal data and can be found within the HUB.

2.3. For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

3. Scope

3.1. The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, on whatever medium. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

3.2. This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

3.3. All members of staff are required to familiarise themselves with the content of this policy and comply with the provisions contained in it. Breach of this policy by staff will be treated as a disciplinary offence which may result in action under the School's *Disciplinary Policy and Procedure*, up to and including summary dismissal depending on the seriousness of the breach.

3.4. This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

3.5. Breach of this policy by others, including Governors, temporary staff, or contractors will be dealt with as deemed appropriate by the Chair of Governors or Headteacher and may be reported to the police.

4. General principles

4.1. All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the School's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

4.2. Staff should discuss with their line manager the appropriate security arrangements for the type of information they access in the course of their work. Contractors, volunteers and interns should discuss this with their primary contact point in the school. The Chair of the Governors is responsible for ensuring that all governors are aware of and respect appropriate security arrangement for information entrusted to them.

4.3. All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption. Data subjects have a right to request information held about them (see Data Protection Policy.) Interns, volunteers and governors should be given access by staff to the information required by them to fulfil their agreed duties and responsibilities.

4.4. All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the IT Department.

4.5. The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the Network Manager unless expressly stated otherwise.

4.6. All staff, volunteers, interns and governors have an obligation to report actual and potential data protection compliance failures to the School Business Leader/ Network Manager who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

4.7. The Data Link Governor will be notified of minor breaches and potential breaches termly, and immediately in the case of a serious breach which may need to be reported to the Information Commissioners Office (ICO).

5. Physical security and procedures

5.1. Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows.

5.2. To avoid unauthorised or accidental access, all paper documents shall be securely locked away at the end of the working day, when they are not being used, or when the room or desk is left unoccupied.

5.3. Available storage cupboards or locked cabinets shall be used to store paper records when not in use.

5.4. Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained.

5.5. Particular care must be taken if documents have to be removed from the school.
5.6. The physical security of buildings and storage systems shall be reviewed on a regular basis. If the security is found to be insufficient, the person discovering this must inform the School Business Leader as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.
5.7. The School carries out regular checks of the buildings and both physical and data storage systems to ensure they are maintained to a high standard.
5.8. The School has an intercom system to minimise the risk of unauthorised people entering the premises and closes the perimeter gates during certain hours to prevent unauthorised access to the grounds. An alarm system is set nightly.
5.9. CCTV Cameras are in use at the School and monitored by the Premises Team. Recordings are made for the safety and protection of those on the site and to aid detection of crime.
5.10. Visitors should be required to sign in at the reception. They must never be left alone in areas where they could have access to confidential information unless such access has been agreed to be necessary to the visit.

6. Computers and IT

Responsibilities of the IT Manager

The IT Network Manager shall be responsible for the following:

6.1. ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;
6.2. ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management;
6.3. along with the Headteacher, ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.
6.4. Furthermore, the IT Network Manager shall be responsible for the following:
6.5. assisting all members of staff in understanding and complying with this policy;
6.6. providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
6.7. ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
6.8. receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];
6.9. taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
6.10. monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
6.11. ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Responsibilities – Members of Staff (including Governors, Interns and Volunteers)

6.12. All users must, at all times comply with all relevant parts of this policy when using the IT Systems.
6.13. Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.
6.14. All users must immediately inform the IT Network Manager of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the *Breach Notification Policy*.
6.15. Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems must be reported to the IT Department immediately.
6.16. Users are not entitled to install onto school systems any software they own, have obtained or provided without permission. Prior to installation, staff must obtain written permission from the IT Network Manager. This permission must clearly state the name of the software, and onto which computer(s) or device(s) it may be installed.
6.17. Furthermore, any such software must be approved by the IT Network Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.
6.18. Physical media (e.g. USB memory sticks or data storage disks of any kind) must be virus-scanned before using it to transfer files. Approval from the IT Network Manager must be obtain prior to transferring of files using external cloud storage systems.
6.19. If a user detects any potential or actual virus, this must be reported immediately to the IT Network Manager (this rule shall apply even where the anti-virus software automatically fixes the problem).

System Access Security

6.20. All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.
6.21. The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teaches individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.
6.22. All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods (e.g., finger prints) can only be used if approved by the IT Department.
6.23. All passwords must, where the software, computer, or device allows:
- be at least 6 characters long including both numbers and letters
- be changed on a regular basis (and at least every 180 days)
- cannot be the same as the previous 10 passwords you have used
- not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.)

6.24. Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the IT Network Manager as appropriate and necessary.
6.25. Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

6.26. Any member of staff who discloses their password to anyone, other than a member of I.T., in the absence of express authorisation will be liable to disciplinary action under the School's *Disciplinary Policy and Procedure*.
6.27. Any member of staff who logs on to a computer using another member of staff's password or accesses the device when it has been left unlocked, will be liable to disciplinary action up to and including summary dismissal for gross misconduct.
6.28. If you forget your password, you should notify the IT Department to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.
6.29. You should not write down passwords if it is possible to remember them. If necessary, you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.
6.30. School computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) must be protected with a screen lock that activates after a period of inactivity. You may not change this time period or disable the lock.
6.31. All mobile devices provided by the School, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not change this time period or disable the lock.

Data security

6.32. Personal data sent over the school network must be encrypted or otherwise secured.
6.33. All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior written authorisation from the IT Network Manager, who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems and opened or run.
6.34. Staff, Governors and visitors may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided the relevant requirements and instructions governing this use are followed.
6.35. All usage of 'own device(s)' whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy). The IT Network Manager may at any time request the immediate disconnection of any such devices without notice.

Electronic storage of data

6.36. All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by the IT Department.
6.37. All data stored electronically on portable physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.
6.38. Staff should not store any personal data on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the Headteacher. Where permission is given, any new or changed data must be copied back onto the School's computer network in order for it to be stored and backed up. Personal data on mobile devices must be deleted as soon as any need for its retention has passed

6.39. All electronic data must be securely backed up by the end of the each working day and is done by the IT Department.

7. Off-site working

7.1. . Where staff are taking confidential information off-site, they must be satisfied that appropriate technical and practical measures are in place at the home or other remote location and on the journey between school and off-site to maintain the continued security and confidentiality of that information.

7.2. When someone has been given permission to take confidential or other information off-site, they must ensure that:

- the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all confidential material that requires disposal is shredded or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.

8. Communications, transfer, internet and email use

8.1. When using the School's IT Systems users are subject to and must comply with the School's *Electronic Information and Communication Systems Policy*.

8.2. The School works to ensure the systems to protect pupils and staff and are reviewed and improved regularly.

8.3. Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee, and the school cannot accept liability for the material accessed or its consequence.

8.4. If staff, visitors or pupils discover unsuitable sites or any material which would be deemed unsuitable or illegal, this should be reported to the Safeguarding Officer or I.T. Network Manager or their team.

8.5. All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by tracked DX (document exchange) or recorded delivery.

8.6. Postal, DX, email addresses and numbers should be checked and verified before information is sent. In particular extra care must be taken when adding email addresses, where auto-complete features may have inserted incorrect addresses or recipients.

8.7. Do not reply to emails using 'reply to all' before checking that everyone on the recipient list should be seeing the reply.

8.8. Do not forward emails without checking if email addresses and personal information in the body of the email need to be deleted or not.

8.9. You should be careful about maintaining confidentiality when speaking in public places.

8.10. Confidential information should be marked 'confidential' and only circulated to those who need to know the information in the course of their work for the School.

8.11. Personal or confidential information should not be removed from the School without prior permission from the Headteacher except where the removal is temporary and necessary. When such permission is given the bearer must take all reasonable steps to ensure that the both the integrity and the confidentiality of the information are maintained. To this end, the information:

- must not transported in see-through or other un-secured bags or cases;

- not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

9. Reporting security breaches

9.1. **All members of staff have an obligation to report actual or potential data protection compliance failures.**

9.2. All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the IT Network Manager.

9.3. When receiving a question or notification of a breach, the IT Network Manager shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

9.4. Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the IT Network Manager. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, IT Network Manager.

9.5. Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the School Business Leader.

9.6. All IT security breaches shall be fully documented and reported termly to the Data Link Governor.

9.7. Full details on how to notify of data breaches are set out in the *Breach Notification Policy*.

10. Related Policies

10.1. Staff should refer to the following policies that are referenced in this *Information Security Policy*:

- Data Breach Policy
- Data Protection Policy