Bow Community Primary School

Information Security Policy

Version 2.0
Document Date: 19th January 2022

Bow Community Primary School
Station Road
Bow
Crediton
EX17 6HU

If you require help in the interpretation of this policy, contact:
Alvin Scott (Data Protection Officer)
Devon Moors Federation
Filleigh Primary School
Castle Hill
Filleigh
Devon
EX32 0RS
dpo@devonmoorsfederation.devon.sch.uk

If this document has been printed, please note that it may not be the most up-to-date version.

For the current version please contact the Clerk to the Governors.

1. Introduction

1.1 This Information Security Policy outlines Bow Community Primary School's approach to information security management relating to electronic and paper-based information. The policy is a demonstration of the school's commitment to protecting information through the robust implementation of appropriate and adequate information security procedures.

1.2 Maintaining the confidentiality, integrity and availability of information, in all its forms, are critical to the functioning of the school. Failure to adequately secure information increases the risk of financial and reputational losses from which could pose a major risk to the viability of the school.

1.3 Effective information security depends on suitable technical measures, appropriate policies and procedures, as well as satisfactory staff training. The school is committed to maintaining a continuous cycle of improvement.

1.4 The Information Security Policy provides the guiding principles and responsibilities necessary to safeguard the security of the school's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

1.5 The objectives of this policy are to:

- Provide a framework for establishing suitable levels of information security for all of the school's information systems and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems
- Assure confidentiality of sensitive and confidential information
- Ensure integrity of data by not allowing unauthorised modifications
- Assure availability of data
- Ensure that appropriate monitoring and reporting processes are put in place to identify and act upon breaches of information security
- Ensure that all school staff understand their own responsibilities for protecting the confidentiality, integrity and availability of the data they handle
- Protect the school from liability or reputational damage.

1.6 The principles defined in this policy will be applied to all of the physical and electronic information assets for which the school is responsible. This policy is applicable to, and will be communicated to, all members of the school's staff. Members of staff will be made aware of this policy at induction.

1.7 Primary responsibility for implementing this policy lies with the head teacher.

2. Associated Policies and Procedures

2.1 This policy should be read in conjunction with the following additional school policies:

- Acceptable Use Of Mobile Phones & Cameras Policy (see Staff Handbook)
- Code of Conduct Policy
- Confidentiality Policy
- Data Protection Policy
- Disciplinary Policy
- E-Safety Policy + E-safety Acceptable Use Policy Guidance
- Information Security Incident Management Policy & Procedure

3. Access Control and Categories of Data

3.1 Information held by the school falls into different levels of security dependant on who should have access to it. No individual should be able to access information to which they do not have a legitimate access right.

3.2 The school has procedures in place to ensure that information is only accessible to the appropriate members of staff. Notwithstanding the systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. The school has a Whistleblowing Policy which sets out how anyone concerned about inappropriate access can approach reporting this. Such unauthorised access would also constitute a data breach that needs to be reported following the school's Information Security Incident Management Policy & Procedure.

3.3 Information Security Level Definitions

Security Level	**Definition**	**Examples**
Sensitive	Normally accessible only to specified members of school staff. By its nature this information needs to be treated with greater care than other personal data.	UK GDPR-defined special categories of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record); safeguarding data; EHCP's and IEPs; Education Psychologist reports; Education Welfare Officer reports; medical records; personnel records; SEN registers; financial records regarding staff pay; staff personnel records, part 2 minutes. Passwords should also be treated as belonging to this category.
Confidential: Personal Data (that identifies individuals)	Normally accessible only to school staff	UK GDPR-defined personal data (information about an identifiable, living individual including: name, home / work address, age, date of birth, telephone number, schools attended, gender, photographs); pupil reports; exam reports;

		draft reports, papers and minutes; internal correspondence, final working group papers and minutes, committee papers.
Confidential: Non-Personal Data (that does not identify individuals)	Normally accessible only to school staff	Lesson plans, curriculum plans, class lists (if only showing initials or forenames)
Public	Accessible to all members of the public	Approved minutes of the governing board, information available on the school's website.

4. Technical Security

4.1 The school will be responsible for ensuring that its infrastructure / network is as secure as is reasonably possible and that:

- network access restrictions are in place to ensure that users can only access data they are authorised to access
- no user is able to access another's files (other than that allowed for monitoring purposes)
- logs are maintained of access by users and of their actions while users of the system
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school's systems and data
- there are regular reviews and audits of the security of school's computer systems
- responsibilities for the management of technical security are clearly assigned to appropriately trained staff
- an appropriate system is in place for users to report any actual / potential technical incident via the DPO (dpo@devonmoorsfederation.devon.sch.uk
- an agreed policy is in place for the provision of temporary access of "guests" e.g. trainee teachers onto the school's system
- Access to SIMS (personal information), FMS and FPS (financial information) and office-based data is restricted to identified individuals through user names and passwords
- an agreed procedure is in place regarding the use of removable media on school devices. All school laptops are encrypted: staff are provided with encrypted memory sticks.
- the school's infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- wherever possible, 'time-out' functions are used which log-out a user after a given time period of inactivity

- appropriate backup procedures are in place to ensure that any lost data can be retrieved. Recovery procedures are tested on a regular basis.

Encryption

4.2 Encryption is a process whereby the data held on a computer is encoded so that it can only be accessed by an authorised user. Once a hard drive has been encrypted, it is not possible to retrieve any data from the drive unless a legitimate user logs in. It is also impossible to access the data by connecting the hard drive to another computer without the correct credentials.

4.3 School laptops will be encrypted if they contain sensitive or confidential information. Any laptops that may be removed from the school and that contain sensitive or confidential data are encrypted. Microsoft Bit Locker is used for this purpose. Servers are not encrypted but are protected by physical security as they are kept in a room which is locked when the school is closed.

4.4 Only encrypted flash memory sticks and external USB hard drives are allowed to be used by staff as part of working for the school. These must not be backed up at home. They should be backed up on the staff member's personal drive on the school's network.

School Wi-Fi Security

4.5 The school has a Wi-Fi network that is used to provide staff and pupil laptops with wireless access to their school's network and the Internet. In order to guard against unauthorised use of this network, it is authenticated and encrypted using WPA2-PSK (TKIP/AES) technology. The network was professionally installed and is maintained, when necessary, by Scomis and RM (SWGFL).

Internet Filtering

4.6 The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The school has an appropriate filtering system in place. However, any filtering system cannot, however, provide a 100% guarantee, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, that filtering should form only one element in a larger strategy for online safety and acceptable use.

4.7 The responsibility for the management of the school's filtering policy is held by RM. They will manage the school's filtering and will keep a record of changes to and breaches of the filtering system.

4.8 Mobile devices that access the school's internet connections (whether school or personal devices) will be subject to the same filtering standards as other devices on the school's systems.

4.9 Any filtering issues discovered by staff should be reported immediately to the filtering provider.

4.10 Requests from school staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded.

4.11 In order to protect data and the integrity of the school's network, staff are requested to report any virus detected immediately to the head teacher.

4.12 Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the head teacher. 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, the head teacher.

4.13 All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from head teacher 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.

5. ICT Inventory

5.1 The school has an accurate and up to date inventory of all ICT assets including mobile devices. An inventory including who it is assigned to is essential when investigating any lost or stolen items. All school equipment is security marked.

6. Password Security

6.1 All school technical systems, including networks, devices and email must be protected by secure passwords to prevent unauthorised access to sensitive or confidential data. Where sensitive data is in use – particularly when accessed on laptops / tablets – the school will consider utilising more secure forms of authentication e.g. two-factor authentication.

6.2 The "master / administrator" passwords for the school's systems used by the technical staff must also be available to the head teacher and kept in a secure place eg a school safe. Consideration should also be given to using two-factor authentication for such accounts.

Staff passwords

6.3 All staff have their own unique username and private passwords to access the school's systems. Staff are responsible for keeping their password(s) private. Passwords must not be shared with anyone other than technical staff under any circumstances, including with supply staff and volunteers. Staff will be made responsible for the security of their username and password and must not allow other staff to access the systems using their log on details. If a password is compromised the head teacher should be notified immediately and the password changed.

6.4 School staff must not log onto a school's network using someone else's username and password. They must also not allow anyone else to use a PC that they are logged in on. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action.

6.5 Staff are requested not to:

- save passwords in web browsers if offered to do so
- use usernames as passwords
- use names as passwords
- send usernames and passwords together
- use their work passwords for their own personal online accounts

6.6 Procedures should be in place so that when a password holder leaves the school any passwords giving that person access to confidential data are changed or that person's account should be inactivated.

6.7 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). If passwords are written down, they should not be kept with the device to which they relate. Passwords should ***never*** be left on display for others to see.

Communicating passwords

6.8 A password should never be communicated in an email that also contains the username for the account to which it relates. The password should be transmitted in a separate message or preferably by another trusted means (e.g. phone call). Before telling anyone the password, ensure that you are communicating with the correct person.

7. Physical Security

7.1. The following physical security solutions are in place to protect data and hardware:

- The server is in a cabinet.
- All administration machines holding personal data are in rooms with restricted access that are locked when the school is closed.
- Computer screens on which sensitive or confidential information is processed or viewed are sited in such a way that they cannot be viewed by unauthorised persons.
- Paper records and documents containing sensitive or 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.
- Hard copies of current staff personnel files are stored in locked cabinets with restricted access in the admin office.
- Safeguarding files are stored online via CPOMS.
- SEN files are kept in a locked cabinet with restricted access in the SECO's room.

- Other confidential information that needs to be retained as hard copies is stored in a secure room that is kept locked at all times.
- An alarm system is set nightly.

8. Procedural Security

8.1 Visitors are required to sign in at the school's reception. They are not left alone in areas where they could have access to sensitive or confidential information.

Laptop Security Procedures

8.2 Members of staff who use school laptops as part of their work are requested to:

- lock the desktop when leaving the laptop unattended for a short time
- shut down the laptop when it will not be in use for a prolonged period
- ensure other people are not watching as passwords are entered
- store their laptop securely

8.3 In addition, staff are requested not to:

- leave laptops unattended unless the security in place is trusted
- use public wireless hotspots as they are not secure
- let other people use their own personal laptop

Memory Cards

8.4 The use of memory cards in cameras means that they will generally be used to store photos and video clips of children. It is not normally possible to encrypt this storage media, so the loss of a school digital camera or video camera off site would mean that these images are at the mercy of whoever finds them. In order to minimise the risk of this happening, staff are advised to wipe the media as soon as possible after pictures have been taken, once the images have been copied to a secure location.

Email Security

8.5 Staff must use their school email (Office 365) account for all emails relating to school matters.

8.6 Staff must not let anyone else use their account nor share their password, in school or at home.

8.7 Sensitive or confidential information sent to recipients external to the school must be encrypted using Egress encryption or a password protected file.

8.8 School staff must:

- use blind carbon copy (Bcc) when emailing more than one external recipient to prevent the inappropriate disclosure of email addresses

- double-check they are using the correct email addresses of recipients prior to sending information to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses
- use the school's contacts or address book in order to help stop email being sent to the wrong address
- be cautious when forwarding emails as they may contain data the new recipient should not see. If an email forms part of an email thread, the whole thread can be forwarded along with an individual email. To avoid forwarding inappropriate data; copy and paste only the content you want to send into a brand new email. This is especially relevant when forwarding an email to a third party
- report any spam or phishing emails to the IT team
- be extremely wary of emails requesting or asking for confirmation of any personal information, such as passwords
- take extreme care with emails from unknown senders, particularly where they contain attachments as these may contain viruses or other forms of malware that may cause loss of data or damage to the computer. If in doubt, do not open any attachments or click on links within the email until the identity of the sender has been verified
- if an email is received that was intended for another person, notify the sender and delete the email. The information it contained must not be used or disclosed to anyone else.

8.9 Staff are required not to:

- forward school emails to a personal email account
- download school emails or their attachments to a non-school computer
- click on links in unsolicited emails
- reply to chain emails.

Camera and Mobile Phone Security

8.10 Staff shall only use cameras and mobile phones owned by the school to capture images at school and on school trips.

8.11 Image files on school cameras should be downloaded onto secure school equipment as soon as possible and deleted from the camera's memory.

8.12 Staff using school cameras and mobile phones must adhere to the requirements of the school's Handbook.

8.13 Parents and volunteers are not permitted to use their own cameras or mobile phones to take photographs on school premises or on school trips.

8.14 A member of staff's personal mobile device can be used to access school emails, however it must be pin / password or similarly protected at all times.

8.15 If any school owned devices (memory sticks, cameras tablets etc.) are lost or stolen it must be reported immediately to a member of the SLT.

8.16 Mobile phones 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 protection with a screen lock that will activate after a period of inactivity. Staff shall not change this this time period or disable the lock.

Printed Personal Data

8.18 School staff must:

- Ensure that at the end of the working day, or when staff leave their desk unoccupied, all paper documents containing sensitive or confidential data is securely locked away to avoid unauthorised access.
- When printing or copying sensitive or confidential material, staff must collect it from the printer as soon as possible and must not leave any such information on the printer.
- Ensure that no sensitive or confidential information other than first name is displayed on classroom walls or in areas where it can be seen by the public.

Distributing Information Securely by Post

8.19 Staff are required to double-check they are using the correct postal address for a recipients prior to sending information to them.

8.20 If you will be sending sensitive data to an address that has not been used for some time the currency of this address should be checked prior to sending the information. The package should be marked as 'Confidential'.

Verbal Communication

8.21 Staff should take appropriate precautions to avoid inappropriate disclosure of sensitive and confidential information during verbal communications. Particular care should be taken in environments where individuals are present who are not employed by the school.

8.22 Conversations involving sensitive information should always take place in a confidential environment where others who should not be privy to such information are not present.

8.23 Staff must be satisfied of the identity of the person to whom they are speaking before disclosing sensitive or confidential information to them. This is particularly important before disclosing information over the telephone.

9. Working from Home

9.1 Staff should not take sensitive or confidential information home without prior permission of the head teacher and should only do so where appropriate technical and practical measures are in place

within the home to maintain the continued security and confidentiality of that information. Staff who have been given permission to take such information home, must ensure that:

a) any hard copies of the information are kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

b) any sensitive or confidential information taken home remains subject to the requirement for secure disposal detailed in the school's Retention and Disposal Policy. For example, hard copies require disposal such as cross-cut shredding.

9.2 Staff working from home must:

- Use only an encrypted device to transport electronic sensitive or confidential information out of school.
- Only use a school provided encrypted drive if a USB flash drive is to be used to transport sensitive or confidential information.
- Ensure that any school laptop taken home is encrypted, unless only remote access is to be used and no school information is stored on the hard drive.
- Ensure that, during transport, the information and equipment is:
    a) kept on your person at all times (e.g. when stopping off on the way home)
    b) be contained appropriately (e.g. in a zipped bag) to reduce the risk of loss or opportunistic theft
- Ensure that family members and other persons not employed by the school do not have access to any electronically stored school data.
- Not download or copy sensitive or confidential data to an unencrypted device (eg laptop or flash drive).
- Not store mobile devices provided by the school in their car.
- Not allow others to use school laptops or USB sticks under any circumstances.

9.3 Sensitive or confidential information taken outside of the school must not:
a) be read in public places (e.g. waiting rooms, cafes, trains, etc.); or
b) left unattended in any place where it is at risk (e.g. in car boots, cafes, etc.).

10. Retention and Disposal of Data

10.1 Data is held for the periods of retention recommended by the Information and Records Management Society and is disposed of in accordance with the school's Retention and Disposal Policy.

11. Data Breaches

11.1. School staff are required to report immediately any data breaches they become aware of to the school's Data Protection Officer (DPO). The DPO will in turn inform the head teacher without delay.

11.2 Data breaches are dealt with in accordance with the school's Information Security Incident Management Policy & Procedure.

11.3 School staff receive training on what constitutes a data breach, how to avoid them and the procedure to follow if one is discovered.

12. Disciplinary Action

12.1. Disciplinary procedures may be instigated if there is evidence to suggest that school staff are disregarding information and data security procedures and, in exceptional circumstances where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

13. Policy Monitoring and Review

13.1 The school undertakes monitoring of compliance with the requirements of this policy on a regular basis and the results of this are reported to the head teacher.

13.2 The school's Data Protection Officer (DPO) will assist the school in such monitoring.

13.3 The school's DPO will review the adequacy of this policy annually and will recommend improvements.

14. Advice and Assistance

14.1 For assistance in interpreting this policy, please contact the school's Data Protection Officer:

Alvin Scott (DPO)

Copplestone Primary School
Bewsley Hill
Copplestone
Crediton
EX17 5NX

Email: dpo@devonmoorsfederation.devon.sch.uk

Policy Date	Summary of Change	Contact	Implementation Date
20/01/2019 19/01/2022	New policy created Policy reviewed & updated to reflect changes consequent to Brexit	The Clerk to the Governors or The Data Protection Officer	