# BLOSSOMFIELD

**Infant and Nursery School**
**(incorporating Blossomfield Childcare)**

# Information Security Policy

**Eastcote Close, Shirley, Solihull**
**West Midlands, B90 3QX**
**Telephone: 0121 744 5522**
**Email: office@blossomfield.solihull.sch.uk**

**Date Reviewed: October 2024**
Reviewed internally for GDPR purposes – no amends made
Approved by Governors on 27 November 2024
**Next Review Date: SMBC review cycle**

**Signatures:**

Olivia Chapman and Sophie Garraty
Chair of Governors Chair of Governors

# CONTENTS


| No | Item | Page |
|---|---|---|
| 1 | Scope | |
| 2 | Key Principles | |
| 3 | Creating, Storing and Managing Information<br><br>3.1 Paper Information<br>3.2 Electronic Information | |
| 4 | Receiving, Sending and Sharing Information<br><br>4.1 Post – receiving and sending<br>4.2 Email – receiving and sending<br>4.3 Telephone Calls<br>4.4 Conversations<br>4.5 Information Sharing/Processing | |
| 5 | Mobile Working | |
| 6 | Premises Security | |
| 7 | Portable Media Devices | |
| 8 | Anti-Malware | |
| 9 | Access Control | |
| 10 | Monitoring System Access and Use | |
| 11 | Potential Breaches of Security or Confidentiality | |

# 1 Scope

This policy applies to:

- All members of staff (including all employees, supply staff, volunteers, work experience and any other individuals working for Blossomfield Infant and Nursery School and/or Blossomfield Childcare ('Blossomfield') on a contractual basis.

The importance of this Policy:

- This Information Security Policy lets you know what your Information Security responsibilities are at Blossomfield. Everyone has a role to play and it is vital that you understand yours.

The objective of the Policy is to:

- Inform Staff and Governors and protect Blossomfield from security issues that might have an adverse impact on the School. Achieving this object will rely on all Staff and Governors of Blossomfield complying with this Policy.

# 2 Key Principles

Blossomfield has adopted the following six principles to underpin its Information Security Policy:

All personal data shall be:

1 processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
2 used for specified, explicit and legitimate purposes ('purpose limitation')
3 used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');
4 accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay ('accuracy');
5 kept no longer than is necessary ('storage limitation'); and
6 processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

# 3 Creating, Storing and Managing Information

Blossomfield has adopted both a clear desk and clear screen policy to reduce the risk of unauthorised access, loss of and damage to information during and outside normal working hours or when work areas and computers are unattended.

The purpose of this section is to establish Blossomfield's requirements to ensure that information is not disclosed by being made available in any form to unauthorised individuals.

## 3.1 Paper Information

- Keep clear desks as this is an obvious way of preventing any confidentiality problems arising from having pupils or other Staff members at desks or disclosure when desks are left unattended. A clear desk will help to protect against the disclosure of information.
- Confidential documents must not be left on display or unsupervised.
- Store confidential information in locked cabinets, returning them to these cabinets when not required.
- Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids.
- Do not leave paper by printers or photocopiers where other people may take it or read accidentally.
- Spoiled photocopies or prints may still be confidential. Do not put in waste paper bin but dispose of them as confidential waste. Always check that originals have been removed from the device as well as copies.
- Dispose of confidential paper by shredding or putting in a confidential waste bag (located in school office). Never dispose of confidential waste in a waste paper bin or other receptacle.
- Destroying information earlier than necessary may be a breach of the law. It is therefore important that retention periods are checked before destroying any records. Please refer to your Data Protection Champion, Linda O'Malley in the school office.

## 3.2 Electronic Information

- All confidential information must be stored on SMBC approved electronic devices or systems with access controlled or restricted. All EICTS supported laptops/machines are automatically encrypted. Any other machines that are used in school must also have encryption to protect any data held.
- Confidential information must not be stored on local unencrypted hard drives.
- Personal data should never be stored on the C: drive of a laptop or PC. If you have a business need to store this information, you must ensure that it is held in a secure system location.
- If confidential information has to be transferred to other portable media, such as USB stick, it must be encrypted with appropriate security software approved by School/SMBC.
- PC screens/laptops/tablets must be sited away from public areas so that pupils and visitors cannot read the screens.

- Portable devices used to conduct face to face meetings should use a school approved platform such as Microsoft Teams, Cloud Parents Evening System etc. Care also needs to be taken by the Staff member in ensuring no confidential or personal data is visible to the other person(s) taking part in the face to face meetings.
- When using Microsoft OneDrive to access and store information on devices, please use caution. Any content you upload to OneDrive, will inherit the sharing permissions of the folder in which you are storing it. For example, if you store content in a public folder, the content will be public and available to everyone on the internet who can find the folder. If you store content in a private folder, the content will remain private. If sharing your content with other users via a link, an email with the link is sent to the other person(s). The link contains an authorisation code that allows anyone with the link to access your content. The person(s) you sent the link to can then forward the link to other people who will also be able to access your content even if you did not choose to share the content with them. These permissions can be revoked by signing into your OneDrive account and selecting the specific content to manage the permission levels.
- When using Microsoft Teams, be aware that your Teams' profile includes information you provided when setting up your Microsoft Account. Your display name and picture will be visible to other users on Teams that have your contact information. If you have given permission, Teams will sync your device contacts periodically and check for other Teams' users that match contacts in your device's address book. You can block users if you do not wish to receive their communications or report a concern to Microsoft. You are also in control of showing your static or live location with individuals or groups in Teams. Push notifications (alerts letting you know of incoming calls/chats etc) are provided by a third party. The company providing the notification service on your device will use this information in accordance with their own Privacy Policy rather than that of Microsoft. More information on this can be sought from your GDPR Champion.
- Revoking permissions for a link effectively de-activates the link.
- Portable ICT devices (eg notebook PCs, handhelds etc) must not be left unattended in any public area.
- Individual user id/passwords must not be shared with anyone, including other Staff members and Governors. You, as an individual, are responsible for all transactions undertaken on SMBC's network using your network ID.
- Passwords must not be written down and left with any equipment or accessible by anyone else.
- Make passwords hard for anyone else by incorporating numbers and mixed cases. Some systems may require this already.
- Locks screens whenever leaving any ICT equipment unattended. This will prevent anyone accessing any restricted information on the equipment whilst unattended.
- Teachers taking the register using SIMS must not display personal or sensitive information on the white board. If you need to access a pupil record, ensure that it is not displayed externally.

- If you discover that you have access to confidential information that you believe should be restricted, you should notify your Data Protection Champion immediately.

# 4 Receiving, Sending and Sharing Information

## 4.1 Post – Receiving and Sending

- Post should be opened and dealt with securely and away from public areas if it contains confidential information. Do not leave unsealed, confidential documents in open post trays or pigeon holes.
- Staff must ensure that any email to an individual marked "Private and Confidential" or "Personal" or any combination, is only passed to the named recipient – unless a prior delegation arrangement has been made.
- If outgoing post contains confidential information to an individual, the envelope should be clearly marked as "Private and Confidential" and to be opened by "Addressee Only". A return address must also be included on the envelope and consideration given to double bagging the package.
- Print each letter separately, making use of any printing security and use window envelopes where possible. Check the address is current and correct. Do not simply copy previous letters. Double check that the letter and papers are for the correct recipient and address.
- When using a mailshot or multiple mailings, have a procedure in place to check that no-one else's personal information is in the wrong envelope. If possible, another person or supervisor should check mailings against address lists and sign off before dispatch.
- Consider using signed for or tracked post if the package contains sensitive or confidential information and/or the volume justifies secure delivery.
- Post containing very high risk/confidential-restricted information, should only be sent to a named person and use of tracked and signed for mail or courier should be used for delivery with signature of receipt.
- If post goes astray or is issued to the incorrect address, notify your Data Protection Champion immediately. If the post contains personal or confidential information you should follow the Security Breach Procedure.

## 4.2 Email and Other Electronic Communications – Receiving and Sending

- Blossomfield does not have total control over incoming emails so staff must be aware of the dangers of opening messages from unknown or untrusted sources. Do not click on links in emails unless you know they are form a trusted source and never provide passwords in response to email requests. If you receive an email that looks untrustworthy, notify the school office immediately so an internal email can be sent around all staff informing them not to open.

- If you are not the intended recipient, the sender should be informed that the message has not reached its intended destination and has been deleted.
- When sending emails, check the email address is the correct one – you may have contacts with similar names. Double check the email is for the correct recipient before sending.
- If sending to a list or group of people, send using 'blind copy' (bcc) so the recipients cannot see each other's email addresses.
- Confidential and Confidential-Restricted information must not be emailed externally using more email unless:
  1. you are using an encrypted email service provided by SMBC; or
  2. the information is encrypted/password protected in an attachment; or
  3. you are sending to an approved email address; or
  4. you are sending to an email address which utilises the same server – eg other Solihull schools/agencies.

- Records of personal data sent by email or other electronic communications (internal or external) are accessible to the data subject if they request access under the GDPR. If a permanent record is required, they should be saved to the appropriate file and the email removed from the email inbox. Do not use personal email as a permanent filing system for pupil, parent or staff records. When a member of staff leaves, the line manager must go through the leaver's emails with them and save any that need to be kept and store appropriately.
- Confidential email must not be forwarded to your own personal email account for private use.

### 4.3 Telephone Calls

- Ensure that you are talking to who you think you are speaking with by verifying their details. It may be appropriate to call them back to verify their credentials.
- If it becomes necessary to leave the phone for any reason, put the caller on hold so that they cannot hear other potentially confidential conversations that may be taking place in the office.

- If you are asked for personal information over the telephone relating to a staff member, pupil or Governor, ask them to email the school from their organisation's/school's office email account so that you may verify their identify and seek consent where necessary from the data subject.
- If the call received or being made is of a confidential or sensitive nature, consider who else may be listening to the conversation. Transfer the caller to a different extension if necessary so the conversation can be continued in a privacy.
- If a message needs to be taken and left on someone else's desk, ensure that the messages do not contain confidential information.
- Do not leave confidential messages on an answer machine as they can be reviewed by people other than the intended person.

### 4.4 Conversations

- Staff should remember that even though they may be on Blossomfield premises, there may be pupils and visitors in the vicinity.
- When having a meeting or interview with someone where confidential information is being discussed, ensure there is sufficient privacy and check the suitability of the room (soundproof?).
- Confidential information should only be discussed with colleagues who need to know the information in order to carry out their job.
- Always consider the surroundings and proximity of others who may be able to hear in public places.

### 4.5 Information Sharing/Processing

- When confidential or personal data is shared with other agencies, for example with local authorities or external providers, then arrangements must be made for that information sharing to be done in a controlled way that meets ethical and legal obligations in one of two ways:
    1. If a service is commissioned with an external provider that needs confidential information to operate, then the contract must contain clauses that list the commissioned organisation's responsibilities for confidential and personal data, including data protection and security. This must include whether the organisation is processing personal data on behalf of Blossomfield or has sole or joint responsibilities for the personal data with Blossomfield. All staff involved in such data commissioning/sharing must be aware of the details of any exiting information sharing agreements/contractual agreements and the obligations that it places on them.
    2. If information has to be shared with another organisation on a regular basis for legal reasons, then this should be done under an information sharing agreement that sets out how the sharing will operate and the standards of management that all parties to the agreement must comply with. Such an agreement will define exactly what information will be shared and how, including the method, transmission or communication between agencies or any shared access security arrangements. The aim is to ensure that appropriate arrangements operate in the participant agencies and ensure the continued confidentiality of shared information. If staff are unclear on what basis information is being shared with another agency, whether an information agreement exists and what obligations that might place on them, it should be clarified with their manager.

## 5 Working away from School

The purpose of this section is to ensure that information and information processing facilities used to access personal and confidential information, are adequately protected with logical, physical and environmental controls.

This includes working away from the School, at home and use of own device to access personal and confidential information.

Work-related information must not be kept at home permanently. Whatever staff are working on or in possession of, work-related information is their responsibility, eg in a school, on the phone, at home, en route to or from school or home, at meetings, conferences etc. If confidential information is handed out in conferences or meetings, the same person is responsible for collecting it back in at the end or ensuring it is only in the possession of those authorised to keep it.

- Only take confidential papers/files with you that you need and keep out of sight in a bag. Do not carry around loose or in clear folders.
- Managers must ensure a log is maintained of which confidential paper files are taken off site, by whom and date they are returned.
- Confidential paper files must be stored securely in a bag or envelope. Best practice is to use electronic files on encrypted devices or access via a secure connection to the network.
- If you have to leave information in cars, lock away paper files and devices in the boot. Do not leave overnight. Take only the equipment/paper/files with you that you need and leave the rest locked away.
- If travelling buy public transport, ensure all your papers, equipment etc are with you when disembarking. Apply the same guidance in 4.3 and 4.4 above with regard to making and receiving telephone calls containing personal information.
- Only school devices may be used. Do not write down passwords. You must not use the 'remember me' function to save user name and password details on the device. Sign out completely after using the system. Any confidential files opened may be downloaded before closing down your device; these need to be deleted from 'downloads'
- When working at home, paper and equipment should be stored and securely after use. Do not leave open confidential files on view and lock your device screen when away from desk. Shut down after use. All confidential information must be safeguarded from access, no matter how unintentional, by anyone who has no need to know – eg family and friends. This would be an unauthorised disclosure. Equipment and information should not be left in the car overnight at home but securely stored in the home. Confidential information must be disposed of at school, not at home. Use strong security on a home Wi-Fi connection.

## 6 Premises Security

- All visitors must sign in and out and disclose who they are visiting. If the visitor is on the Local Authority's list of approved workers, they do not need to show their DBS but their official SMBC ID badge will suffice. If they do not have this with them, they will be denied entrance.
- Visitors with an SMBC ID badge are permitted to move around school unescorted unless this is their first visit to school.
- Other visitors will be required to wear a school ID Visitor Badge at all times whilst on site and will be escorted by a member around school.
- Staff should challenge anyone in school that are unknown to them, are unaccompanied by a member of staff or are not wearing an ID badge.

- Staff should be aware of anyone they do not known attempting to follow them through a security gate/door and if appropriate, escort them back to reception.
- Managers should ensure that all paper based or electronic records are adequately protected. Risk assessments should identify any potential threats and an appropriate risk management strategy should be produced.
- Parents and others who do not want to discuss private matters with a receptionist in a public area should be offered the opportunity to be seen elsewhere.

## 7 Portable Media Devices

The purpose of this section is to establish control requirements for the use of removable media devices within and across Blossomfield. Portable media devices include, but are not limited to, USB sticks and memory cards.

- Connection of non-Blossomfield supplied removable media devices to the Blossomfield computing infrastructure is only permitted for the purpose of reading files from the device. Blossomfield files must not be written to a non-Blossomfield supplied device.
- Staff must not alter or disable any controls applied to any computing device by SMBC IT Service as part of the deployment of a removable media device.
- Removable media devices must not be used for the primary long- term storage of Blossomfield information.
- All information classified as ‘confidential’ or ‘personal’ that is stored on a removable device must be encrypted.
- Passwords applied to encrypted devices must conform to the minimum standard required stated in section 3.2 (Electronic Information) of this Policy.

## 8 Anti-Malware

The purpose of this section is to establish requirements which must be met by all devices within Blossomfield’s/SMBC’s computing infrastructure, to protect the confidentiality, integrity and availability of Blossomfield’s/SMBC’s software and information assets from the effects of malware.

- Unless undertaken by or following instruction from IT staff, staff must not disable anti-malware software running on, or prevent updates being applied to devices.
- The intentional introduction of viruses to Blossomfield’s/SMBC’s infrastructure will be regarded as a serious disciplinary matter.
- Only software that has been authorised by Blossomfield/SMBC can be installed upon Blossomfield’s systems.
- Each member of staff is responsible for immediately reporting any abnormal behaviour of Blossomfield’s/SMBC’s computing systems to the IT Service Desk.

- Prior to any encryption, all files must be scanned for and cleaned of viruses before being sent to any third party.

## 9 Access Control

- Access to information shall be restricted to users who have an authorised need to access the information.
- Users of information will have no more access privileges than necessary to be able to fulfil their role.
- All requests for access to Blossomfield/SMBC computer systems must be via a formal request to your line manager.
- Blossomfield reserves the right to revoke access to any or all of its computer systems at any time.
- Users must not circumvent the permissions granted to their accounts in order to gain unauthorised access to information resources.
- Access to the internet by a visitor to school will only be given at the discretion of the Headteacher.
- Users must not allow anyone else to use their account or to use their computers while logged in with their account.
- Computer screens should be 'locked' or the user logged out before leaving any workstation or device unattended.
- Users should not leave workstations or devices in 'sleep mode' for convenience.

## 10 Monitoring System Access and Use

The purpose of this section is to establish control requirements for the monitoring and logging of information security related events relating to the use of Blossomfield's information and information systems.

System access and staff data use is monitored by the Local Authority on a regular basis in order to address any possible breaches of Policy. The Headteacher is alerted by the Authority if there is a suspected case of mis-use (eg someone accessing inappropriate websites). The Headteacher will address this directly with the appropriate member of staff/visitor etc.

Any monitoring will be undertaken in accordance with the Human Rights Act and any other applicable law.

## 11 Potential Breaches of Security and Confidentiality

If staff become aware that information has not been handled according to procedure and there is a data breach or potential security incident, they must report it immediately to their line manager or Data Protection Champion, Linda O'Malley, School Office.

If you are unsure if an incident is a security breach, speak to your line manager or Data Protection Champion as soon as possible and in any event within four hours.

For loss of equipment or if you believe your email or the network may be at risk, contact the Data Protection Champion.

If equipment or confidential information has been stolen, report to the Police and obtain a crime reference number.

Follow Blossomfield's Personal Data Breach procedure for ensuring the incident is reported and recorded appropriately and promptly. This has been supplied to all staff but can also be found at the back of the Data Protection Policy.

## 12 Review

This Policy will be reviewed and updated as necessary to reflect best practice or amendments made to Data Protection Law.

**This Policy should be read in conjunction the School's:**

- Data Protection Policy
- Code of Employee Conduct Policy
- Safeguarding Policy
- School use of Personal, Social Communication Tools
- Use of Mobile Phones and Image Capturing Devices
- Freedom of Information Policy
- Confidentiality Policy
- Personal Data Breach Procedure

**This Policy should also be read in conjunction with SMBC's Policies:**

- Information Security Policy – Mobile Working and Working from Home – Aug 2020
- Information Security Policy – Using Portable ICT Equipment/Media – Aug 2020