Caroline Chisholm School

Ambition Confidence Success

Everyone Every Lesson Every Opportunity

GDPR Information security policy

Author:	
Approval:	Trust board
Date approved:	20/09/2023
Review date:	20/09/2024
Review timescale:	Annual
Keywords:	GDPR Data Information
[Comments]	

Contents

1 Scope

This policy applies to:

- All members of staff, and Trustees; "Staff" includes all employees, locum staff, volunteers, work experience and any other individuals working for Caroline Chisholm School on a contractual basis.

The importance of this policy:

- This Information Security Policy lets you know what your information security responsibilities are at Caroline Chisholm School; everyone has a role to play and it's vital you understand yours.

The objective of this policy is to:

- Inform staff, and Trustees and protect Caroline Chisholm School from security issues that might have an adverse impact on our organisation. Achieving this objective will rely on all staff, and Trustees of the Caroline Chisholm School complying with this policy.

2 Key principles

The Caroline Chisholm School 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 are inaccurate, are erased or rectified without delay ('accuracy');
5) kept no longer than is necessary ('storage limitation');
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

The school 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 the school'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 it accidentally.
- Spoiled photocopies and prints may still be confidential. Do not put them straight into the wastepaper bin, 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 put in a confidential waste bag and follow confidential waste disposal procedure. Do not dispose of confidential waste in a wastepaper bin or anywhere else.
- Destroying information earlier than necessary may be a breach of the law so it is important that retention periods are checked before destroying any records.

3.2 Electronic information

- All confidential information must be stored on school approved electronic devices or systems with access controlled/restricted, e.g., the school network, Office 365 with appropriate restricted access and school approved systems.
- Confidential information must not be stored on local unencrypted hard drives.
- If confidential information has to be transferred to other portable media, such as USB stick or memory cards, it must be encrypted with appropriate security software approved by the school.
- PC screens/laptops/tablets must be sited away from public areas so that pupils and visitors cannot read the screens, e.g., through windows or while waiting in public areas.
- Notebook PCs, handhelds or any other portable ICT device must not be left unattended in any public area (see Mobile Computing below).
- Individual user ID/passwords must not be shared with anyone, including other staff members and Trustees and do not use anyone else's password. You as an individual are responsible for all transactions undertaken on the school's network and associated systems 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 to guess by incorporating numbers and mixed case into it. Some systems will force this already.
- Lock screens whenever leaving any ICT equipment unattended. This will prevent anyone accessing any restricted information on the equipment while it is unattended.
- If you find you have access to confidential information that you believe should be restricted, you should notify school immediately.

4 Receiving, sending and sharing information

4.1 Post – receiving and sending

- Post should be opened and dealt with away from public areas and securely, if dealing with confidential information. Do not leave unsealed confidential documents in open post trays and 'pigeonholes'.
- Staff must ensure that any mail to an individual marked: Private, 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 marked as 'Private and confidential' and 'to be opened by addressee only'. A return address must be shown on the envelope and you should consider double bagging the package.
- Print each letter separately making use of any printing security and use window envelopes. Check the address is the current, correct one – don't 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 you haven't included anyone else's personal information in the wrong envelope. Another person or supervisor should check mailings against address lists and sign-off before dispatch.
- Consider using signed for/tracked post, if it contains sensitive or confidential documents 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 a courier to deliver to the named person with signature of receipt.
- If post goes astray or is issued to the incorrect address, notify your line manager immediately and if the information contains personal or confidential information report using the security incident procedure.

4.2 Emailing and other electronic communications (e.g., text messages) – Receiving and sending

- The school does not have total control over emails received, 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 from a trusted source and never provide passwords in response to email requests.
- 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.
- Check the email address is the correct one – there are staff with similar names and your email contacts will also have external email contacts. Double check that the email is for the correct recipient before sending.
- If sending to a list/group of parents or others, send using 'blind copy' (bcc) so the recipients are not copied into a large list. This especially applies to mailshots.

- Confidential and confidential-restricted information must not be emailed externally using normal email unless;
    a) you are using an encrypted email service provided by the school, or
    b) the information is encrypted / password protected in an attachment, or
    c) you are sending to an approved school email address, or
- 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 or moves to another job, the line manager must go through the Leavers Checklist and save and secure any emails needed to be kept as Caroline Chisholm School records.
- Caroline Chisholm School 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 going on in the office.
- If the call received or being made is of a confidential or sensitive nature, consider who else may be listening to the conversation.
- If a message needs to be taken and left on someone's desk, ensure that these messages do not themselves contain confidential information.
- Do not leave confidential messages on an answer machine as these can be reviewed by people other than the intended person.

4.4 Conversations

Staff should remember that even though they may be on school premises, there may be pupils and visitors around.

- When having a meeting or interview with someone where confidential information will be discussed, ensure that there is sufficient privacy. Check that the room is suitable.
- Confidential information should only be discussed with colleagues who need to know the information in order to carry out their job.
- Always consider your surroundings and the 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 Caroline Chisholm School or has sole or joint responsibilities for the personal data with Caroline Chisholm School. All staff involved in such data commissioning/sharing must be aware of the details of any existing 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.
3. If staff wish to acquire services from any external third parties which involves sharing personal data i.e. setting up new applications/software or engaging with extra-curricular clubs, they should contact Anitha Regupathy, Network Manager, IT department to ensure that the relevant agreements and assurances are in place, before beginning to share any data with the third party in question.

5 Mobile working

The purpose of this section is to ensure that information assets 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 devices to access personal and confidential information.

Work-related information must not be kept permanently at home. Wherever staff are working on, or in possession of, work-related information they are responsible for it, e.g. in 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 hands of those authorised to keep it.

- Take only the confidential papers/files with you that you need and keep out of sight in a bag, do not carry around loose or in clear folder.
- Managers must ensure a log is kept of which confidential paper case files/records staff are taking from school and when they are returned.

- Store confidential paper files/records securely in an envelope or bag. Try to use electronic files on an encrypted device or access via secure connection to the network or approved storage location instead.
- Keeping information in cars: lock away paper files and equipment (laptop/notebook) in the boot, do not leave overnight. Take only the equipment/papers/files with you that you need, leave rest locked away.
- Travelling by public transport: make sure you take all information and equipment when leaving. Be aware of conversations on mobile phone about personal and confidential information.
- Use of laptops: Only school issued devices may be used. Do not write down passwords/pin numbers. You must not use the 'remember me' option to save user and password details on your device when accessing school systems. Make sure these are unticked and sign out/logout after using a system. Do not save login or passwords if asked. Remember any confidential files opened may be downloaded before closing down your device, so delete them from 'downloads'. If files are not accessed directly from Office 365 or remote desktop, then all confidential files must be stored and accessed locally via a school approved encrypted media.
- Working at home: Store paper and equipment securely after use, as you would your own personal valuables. Don't leave open confidential files on a table. Lock screen on laptop/tablet and close down after use. All confidential information must be safeguarded from access, no matter how unintentional, by anyone who has no need to know such as family and friends. This would be an unauthorised disclosure. Don't leave any Caroline Chisholm School equipment or information in a car overnight at home, bring into the house and secure. Don't bin confidential information at home, bring back into an office for confidential waste disposal.

6 Premises security

- All staff must wear their ID badge on school premises and report losses or thefts immediately to the HR Team and, if needed, obtain a temporary visitor badge.
- Make sure that all visitors sign in and out at all times and disclose who they are coming to see. Visitors should be supervised at all times and display a visitor/contractor ID badge.
- Staff should be encouraged to challenge anyone in the school if they do not know who they are, e.g. if they are not accompanied by a member of staff or they are not wearing an ID badge.
- Staff should be aware of anyone they do not know attempting to follow them through a security door and if appropriate be prepared to escort them back to reception if necessary.
- Managers should ensure that all paper-based records and any records held on computers are adequately protected.
- Parents and others who do not want to discuss their 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 the school. Portable media devices include but are not limited to USB sticks or memory cards.

- Connection of removable media devices to the school's network infrastructure is only permitted for the purpose of reading files from the device; files cannot be written to the device unless encryption is chosen.
- Staff must not alter or disable any controls applied to any computing device by the school's 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 school information.
- All information classified as 'confidential' or 'personal' that is stored on a removable media 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 Caroline Chisholm School's computing infrastructure, to protect the confidentiality, integrity and availability of Caroline Chisholm School software and information assets from the effects of malware.

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

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 school network systems must be via a formal request to the HR Team.
- The school 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.

- Users must not allow anyone else to use their account or 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.
- If users find that they have been granted permissions beyond what is necessary, they should inform their line manager and Anitha Regupathy, Network Manager, IT department immediately.

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 school's information and information systems.

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. The school will put in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy.

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

11 Potential breaches of security or confidentiality

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it to their manager immediately.

For losses of equipment or if you believe your email or the network may be at risk, contact the IT Helpdesk immediately via email or 01604 272555 and leave a message if needed.

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