Caroline Chisholm School

Ambition Confidence Success

Everyone Every Lesson Every Opportunity

ICT Acceptable use policy

Author:	Porsha McTaggart
Approval:	David James
Date approved:	01/07/2022
Review date:	30/06/2023
Review timescale:	Annual
Keywords:	ICT Acceptance
[Comments]	

Contents

1 Introduction

This policy is based on government guidance on the acceptable use of ICT systems. It has been agreed by the senior management and approved by the Trustees. The policy will be implemented by all staff and students and will be monitored by the Network Manager and the Principal.

Due to the nature of the internet, social media and advancements in digital technology, it is accepted that there is no technical solution that can consistently guarantee to prevent the misuse of ICT, cyber-bullying or access to unwanted internet material. Caroline Chisholm School will not accept liability for the material accessed or any consequences of Internet access thereof.

However, such circumstances will be carefully monitored, recorded, and dealt with in accordance with this policy. Caroline Chisholm School treats e-safety as an important aspect of education and encourages parental involvement in implementing this policy. Microsoft Intune is the school's device management, and Senso is the school's device monitoring system are both used to protect students and staff from the risks associated with the use of the internet and ICT systems.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching students safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

This policy contains the following important documents:

- Student Acceptable Use Policy
- Device Loan Agreement
- Staff IT User Policy
- Staff Email and Internet Protocol

1.1 Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

2 The importance of digital learning at Caroline Chisholm School

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should always have an entitlement to safe internet access.

Through consistent cross-curricular use, students can become autonomous users of ICT, enabling them to take an active role in their own learning by accessing and applying a range of digital resources. ICT skills and facilities are used to support personalised learning, providing access for the whole learning community to a wide variety of resources. ICT enables students to produce high quality, innovative learning using arrange of multimedia resources.

The educational benefits of all students having Winbooks are considerable. The device presents huge opportunities for exciting and productive activities in lessons across the curriculum as well as enabling more effective independent study and better communication between teachers and students. We recognise that developing high-performing learning habits is critical to student success and that by having easy access to digital technology, students can use the varied learning tools and online resources available to help them reach their full potential.

2.1 ICT for management and leadership

An integrated ICT-based administration and management information system (MIS) provides staff with access to:

- Assessment data to support individual and group target setting and personalised learning
- Electronic registration and attendance recording
- Timetabling and scheduling
- Reporting to parents and carers (both electronically and on paper if required)
- Financial management, budgeting, and forecasting
- Library administration
- DfE returns
- Smart cards (access control, cashless vending, registrations, library, transport payment, system logon, equipment allocation, personal details etc.)
- Provision of online services -assignment submission, Internet, email etc
- Student evaluations -reporting, assignment feedback
- Inventory management -consumables, hardware etc.
- catering
- Personnel -application forms, recruitment, reference checking, Ofsted staff evaluation etc.
- Examinations
- Student and staff details (address, contact details, medical notes etc.)
- Payroll
- Performance measurement and management
- Resource management and booking
- Supplier contract management
- Printer management

Staff training and continuing professional development are available to ensure all staff can make the best use of the ICT resources within Caroline Chisholm School. This is an ongoing programme, reflecting the inevitable developments in technology and the curriculum. A vital aspect of this training is the induction given to new staff to support them in accessing and using the ICT system fully and effectively.

2.2 Internet safety and management

Sophos Filtering is deployed across the network and enables a safer, digital learning environment with real-time, content-aware and granular control web filtering. The filtering service protects students from harmful content while providing the freedom to learn without limits and preventing the blocking of unreasonable restrictions. We have several layers of protection:

- Real-time dynamic content analysis - Keeps users safe by categorising new and existing content in real-time by analysing the content, context and construction of each page
- Granular controls - Build web filtering policies based on user group, content category, location IP and time
- Social media controls - Allows read-only access and removes inappropriate content across social media sites
- Safeguarding - The built-in safeguarding reporting suite notifies us of any safeguarding risks with predefined category rules, including self-harm, suicide, and radicalisation.

2.3 ICT for the Whole Learning Community

Collaborative learning and innovative teaching and learning approaches are facilitated by the VLE. This allows students, staff, parents and, in some cases, the local community to learn together and share learning resources.

Students, parents and carers are able to access learning resources and personal work from home. ICT is central to the involvement of parents and carers in their children's learning. Support for the development of parents' own ICT skills is provided on request by the school, together with online support from teachers and other staff. Links are formed with local primary and secondary schools and further and higher education institutions to make education and facilities available to their students.

ICT provides a range of methods of communication which can be used to establish stronger community links and support youth inclusion and mentoring. Online discussion groups, special interest forums, one-to-one email, and instant messaging can be used to enhance student-mentor relationships. ICT can also support peer-mentoring and provide students with opportunities to extend their experiences through communication with community partners and students in other schools.

2.4 Infrastructure

Computers

A range of desktops, laptops and Surface Gos are provided. This affords versatile and flexible use of ICT across the curriculum and throughout the school. All students are issued with Winbooks, which provides touch-screen interaction.

Peripherals

Printers are situated throughout the primary and secondary phases of Caroline Chisholm School. Access to a wide range of digital devices is available to students and staff. These include digital cameras, digital video cameras, sound recording equipment, scanners, graphics tablets, wireless keyboards, interactive input devices and video conferencing facilities.

Presentation Technology

There is a whole school PA system capable of broadcasting to most areas.

Networking

There is network access throughout the school site, comprising hard-wired and wireless access. The networks provide secure access to all authorised users. Levels of access to curriculum materials, management and administration tools are allocated to users appropriately.

2.5 Technical support

A Network Manager leads the strategic development of the ICT network. This colleague oversees technical maintenance and manages the ICT network team. On-site technical support is permanently available. This is delivered by technicians employed directly by the school and, in some cases, by technical staff employed by our managed service provider.

2.6 Security: Student and Staff Protocol

Students have use of the school's computer systems and internet as part of their curriculum provision. All students are issued a code of conduct to ensure the correct use of these systems. Students and their parents/carers will be required to sign agreements to adhere to the school's rules on the use of computer systems and the internet. The expectations for the use of IT systems and equipment by school staff are set out in the IT User Policy. All staff are given a copy of this policy and are expected to abide by its contents.

2.7 Sustainability and Futureproofing

The school has a strategy for investing in additional ICT equipment to support growing student numbers. This strategy also incorporates the need to replace equipment as it wears out or becomes obsolete.

A sum to support ICT expansion and replacement will be identified in the school's annual budget. The ICT hardware budget will be subject to year-on-year variation depending upon the school's spending priorities.

Network cabling and associated utilities have been installed to formulate maximum flexibility in developing the ICT provision.

3 Student Acceptable Use Agreement

This Acceptable Use Policy is intended to ensure that:

- Young people will be responsible users and stay safe while using the internet, email and other digital technologies for educational, personal and recreational use.
- The school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will ensure that students have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. To do this, students need to understand the rules and systems that are in place to protect them, to ensure that our school system is secure and that no one is subject to bullying or abuse.

3.1 Acceptable Use Policy Agreement

I understand that I must responsibly use school ICT systems to ensure that there is no risk to my safety or the safety and security of the ICT systems and other users. This policy covers all computers, laptops, and electronic devices within the school (irrespective of who owns the device and how the IT system is accessed, e.g., via remote access). Breaches of the agreement usually result in a ban from the use of the ICT facilities and appropriate action being taken under the Caroline Chisholm School behaviour policy where necessary. Please note that users of the IT system may be held liable for costs incurred for repair and/or replacement of equipment where the damage was caused by misuse.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications that are used within Caroline Chisholm School.
- I understand that school staff will monitor/access the screens of students and their user accounts.
- I will keep my username and password safe and secure–I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of 'stranger danger', when I am communicating online.
- I will not disclose or share too much personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people offline that I have communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I will only use the internet in school when being supervised by an adult

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for online gaming, online gambling, online chat rooms, internet shopping, file sharing, or posting videos (e.g., YouTube) unless I have the permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission.
- I will be polite and responsible when communicating with others, I will not use strong, aggressive, or inappropriate language, and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission or email private information about another person, which may put them at risk of any kind.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files I will only use my own personal devices (mobile phones/tablets etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials. Staff have the right to decide what they consider to be inappropriate and offensive.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not make deliberate attempts to damage, graffiti or disrupt any computer systems or equipment, for example: unplugging any cables or attempting to change any system settings. It is unacceptable for a student to switch off another student's machine (this causes not only loss of work but could potentially damage the school computer as well).
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device or attempt to install one via any portable device.
- I will not try to alter computer settings or access, delete or copy school data that I haven't been given permission to use.
- If I mistakenly access inappropriate information on the Internet, I will immediately tell my teacher, or another member of staff. This may protect me against a claim that I have intentionally violated this policy.
- I will not send emails which could cause offence to others. I must not access emails in school which contain material that could be considered inappropriate or offensive. If I have any doubts about emails sent to me, I should not access them.
- I will not remove any ICT equipment from its position without permission from a member of staff. •I will avoid unnecessary printing
- I will not intentionally introduce computer viruses to the school network system.
- I will immediately notify my teacher or the IT technicians if I have identified a possible security problem. I will not go looking for security problems because this may be viewed as an illegal attempt to gain access.
- I will not use social media sites unless granted permission by a member of staff.
- I will not use any camera/camcorder facilities on a mobile phone/camera during the school day unless this is part of a learning activity or authorised by a member of staff.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include:
- Warning from class teacher/performance leader/curriculum support
- Reduced access to the Internet for one or more lessons/after-school facilities
- Detention/Internal Exclusion
- Letter to parent/guardian/meeting with parent/guardian to re-sign Internet use agreement
- Subsequent incidents will be treated very seriously by the principal and may result in exclusion and/or police involvement in the event of illegal activities.

Recording on school property

I understand that I must gain permission from the principal if audio/video recordings are made anywhere on school grounds, it is not linked to school work and the aim is to share on the internet or other communication technologies (phones/tablets etc.) which could affect the school's reputation. This could be in the form of videos posted to websites like YouTube or Twitter amongst others. All material recorded should not discriminate against anybody and should be respectful in nature.

3.2 Consent

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices and Microsoft 365 (both in and out of school)
- I use my own devices in the school (when allowed) e.g., mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school community e.g., communicating with other members of the school (staff or other students), using social media such as Facebook, Snapchat, Twitter, and Instagram etc. as well as school managed email and school social media accounts/website.

Student name:	
Form:	
Signature:	
Date:	

4 Device Loan Agreement

4.1 This agreement is between:

1) Caroline Chisholm School, Wooldale Centre for Learning, Wooldale Rd, Northampton NN4 6TP ("the school")

2) Name of parent:_____ Address:_____("the parent" and "I")

And governs the use and care of devices assigned to the parent's child (the "student"). This agreement covers the period from the date the device is issued through to the return date of the device to the school. All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the student a Winbook ("the equipment") for the purpose of doing schoolwork; Caroline Chisholm School remains the owner of the device.

2. This agreement sets the conditions for students using the loaned Winbook ("the equipment").

I confirm that I have read the terms and conditions set out in the agreement, and my signature at the end of this agreement confirms that I and the student will adhere to the terms of the loan.

4.2 Damage/loss

By signing this agreement, I agree to take full responsibility for the loan equipment issued to the student, and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the student are responsible for the equipment at all times, whether on the school's property or not. If the equipment is damaged, lost or stolen, I will immediately curriculum support in person and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment.

If the equipment is stolen, I will also immediately inform the police. I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas. I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas.

4.3 Device storage

The Winbooks are to remain on-site; I agree that my child will charge the device in its allocated locker at the end of each school day and not take it home.

4.4 Unacceptable use

By signing this agreement, I agree to take full responsibility for the loan equipment issued to the student and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I am aware that the school monitors the student's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'. This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to the Winbook, ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the student, in line with Caroline Chisholm School's Behaviour Policy, if the student engages in any of the above at any time.

4.5 Personal use

The equipment is for the sole user to whom it has been allocated. I agree that the student will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

4.6 Data protection

I agree to take the following measures to keep the data on the device protected:

- Keep the equipment password-protected - strong passwords with a combination of upper and lower-case letters, numbers
- Make sure my child locks the equipment if it is left inactive for a period of time
- Do not share the equipment among family or friends
- Install the latest updates to operating systems, as prompted

4.7 Return date

I will return the device in its original condition to the school office within 7 days of being requested to do so. I will ensure the return of the equipment to the school if the student no longer attends the school.

4.8 Acceptable use

The use of the loaned equipment is covered by the school's acceptable use policy. The loan of the Winbook is conditional on signing and agreeing both this loan device agreement and student acceptable use agreement.

4.9 Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

Student name:	
Parent name:	
Signature:	
Date:	

5 Staff IT User Policy

The purpose of the policy is:

- To outline the acceptable use of computer equipment at Caroline Chisholm School.
- To put in place rules to protect both the user and Caroline Chisholm School.
- To safeguard the system from potential threats such as virus attacks, hacking, system failure and breach of legal requirements.
- To raise staff awareness of their duty to use Caroline Chisholm School's ICT resources for professional purposes responsibly, ethically, and lawfully, and to ensure their students do the same.

5.1 All staff need to be aware that:

- The Network Manager and Senior Leadership Team reserve the right to access files, folders, network data and workstations at any time, with reasonable cause.
- Caroline Chisholm School filters, monitors and records all ICT usage and activity both in school and on school cloud-based software. This includes the use of the internet as well as general network usage. Staff may request that certain sites be temporarily 'unblocked' if this will assist their teaching.
- Staff will have access to Caroline Chisholm School's ICT resources (including their email account) until the final day of their employment by the school.
- External storage devices such as USB sticks are not permitted in school for network security reasons.
- If you have any concerns about the provenance of an email, do not open it, rather delete it and report it to IT Support.
- This policy should be read in conjunction with the school's safeguarding policy.

5.2 Staff need to:

- Be fully aware of the contents of the Student Acceptable Use Policy and do everything they can to ensure it is upheld.
- Use the network and all ICT equipment appropriately and responsibly.
- Report any loss or damage to ICT equipment to the Network Manager immediately.
- Contact a member of the IT Support staff if any resource behaves unexpectedly.
- Be aware that if they install software on a home computer which is licensed through the school, it is their responsibility to uninstall it when they leave the school's employment.
- Be responsible with the amount of storage space used, and to undertake regular 'housekeeping' to delete unwanted files.
- Take care when choosing passwords in order to keep the school's ICT systems secure. Carelessness when choosing passwords leaves confidential student data vulnerable to theft. It is recommended to update your Passwords at the beginning of every term and should contain a mixture of alphabetical, numeric and special characters. We recommend that you change your password at the beginning and end of each holiday to avoid being locked out of school systems.
- Ensure that printing is carried out in a responsible and economical fashion. Where possible use laptops or other electronic means to view documents rather than printing hard copies. When printing is required, duplex monochrome copies should be used. Colour printing should only be used in exceptional circumstances. All printing for classroom use should be sent to reprographics in good time. Personal printing is not permitted.

5.3 Staff must take care not to:

- Harm, offend or bully anyone using ICT.
- Procure, display or distribute any material that may be illegal, harmful, offensive or detrimental to anyone. This includes, for example: racist or extremist material, material of a sexual nature and viruses.
- Engage in any illegal activities.
- Make any sort of recording, whether audio or visual, of any conversation or meeting with anyone in the school community without their express permission, as so doing would constitute a breach of trust.

- Log on using another person's username and password, attempt to access another person's files or data or give out any usernames or passwords.
- Give out, or publish, personal details relating to any member of the school community without permission.
- Take part in any activity that may be detrimental to the school's name, at home or in school.
- Install or run any unapproved or unlicensed software/programs on any school computers, laptops or Surface Pro's.
- Change any of the configuration settings of any school computer, laptop or Surface Pro.
- Provide access to copyright works beyond that which is allowed under current copyright legislation.
- Whilst in school, use personal ICT equipment – whether using the school Wi-Fi network or their own provider's 3G or 4G network, including mobile, hand-held and tablet devices, in a way which contravenes this policy

5.4 Electronic Communication

- Staff must not contact or communicate with any students or parents or carry out any school business using personal social media accounts such as Facebook.
- Professional messaging groups, such as Microsoft Teams should only be set up and managed by a member of staff for school business. These groups should remain unlocked and should be actively monitored and managed by the member of staff responsible. Personal messaging groups such as WhatsApp should not be used for school activities.
- Staff must not engage in personal on-line conversations using the school's network, or access Instant Messaging sites or Chat Sites for personal use whilst in school.
- Staff must maintain the securest settings on any personal social media sites, so that students, parents, former students, and others cannot see any personal information. Staff should not become 'Friends', 'Follow' or make direct connections on any social media sites with present students. This also applies to ex-students until they are 18 and have finished secondary education. Staff are strongly advised to use these sites in a professional manner and, should any concerns arise, they should seek the advice of the principal as soon as possible.

5.5 When accessing the network from outside the School staff must not:

- Transfer any material that could be deemed offensive, harmful, or illegal from outside the school to the school network. This includes transfer by Internet or by any form of removable media.
- Share any confidential or whole school documentation, such as that on the Shared Team sites (For Example: CCS Staff and Faculty team sites), with anyone from outside the school.
- Transfer or store any confidential information on cloud services such as Dropbox or Google Drive. The only cloud storage that may be used is the school provided OneDrive account.

5.6 When using a device provided by the school staff must:

- Adhere to this policy, as above.
- Store the school laptop or Surface Go in an appropriate manner minimising the risk of theft or damage. If left in an unattended motor vehicle it must be concealed in a locked boot.
- Not install programs for which the school does not have a valid licence.
- The loaned device must remain in the possession of staff, should only be used by them and should be securely stored when not in use. All associated items, including the charging cable and Pen inputs, if issued (For example: Apple Pencil, Surface Go Pen and Winbook Pen), should be kept in good order. Staff must be mindful of the agreement they signed when their Loaned device was issued and ensure that any loss or damage should be reported to the IT Manager immediately.
- If staff leave the employment of the school, or have an extended leave of absence e.g., for maternity/paternity leave, then the loaned device must be returned to IT Support prior to their official leaving/period of absence date.
- Personal photographs or video should not be stored on the Loaned device.

- Where photos or videos have been taken of students using a school Loaned device for the purpose of teaching and learning these should not be retained for any longer than absolutely necessary.
- Any confidential student data stored on staff's Loaned devices must be deleted once it is no longer needed.
- Staff Loaned devices are configured by the School Mobile Device Management System. Staff must not attempt to change these settings or remove it from the Management System.
- VPN (Virtual Private Network) apps must not be used.
- Should the Loaned device be left unattended, and it is stolen from a staff member's home, car or other establishments., staff will be responsible for its replacement.
- Remember that any connection cost incurred by accessing the internet from outside school is not chargeable to the school.
- Loaned devices may be checked periodically for safety and compliance with school policies. Outcomes will be reported to the Head.
- Paid iOS Apps should be purchased through the school by contacting IT support. Any Apps purchased by staff independently of this will not be reimbursed. When requesting that an App be purchased, authorisation should be sought from the relevant Head of faculty. The cost of purchased Apps will be taken from departmental budgets.
- Social Networking Apps should not be downloaded or installed, unless for a specific and authorised purpose.

6 Staff Email and Internet Protocol

This protocol sets out the purpose for which email, and Internet facilities are made available to staff, and it applies to all employees, whether temporary or permanent. You must always observe this protocol and should know non-compliance may result in disciplinary action up to and including summary dismissal. This protocol is to be read in conjunction with the security section of the Staff Handbook.

6.1 Use of the Email System

Business use

The email system is provided for the business purposes of the Caroline Chisholm School and should be primarily used for that purpose. The school permits personal use of the email system, but only where such use is limited, does not interfere with the performance of your duties and does not adversely affect the email system. "Limited" in this sense means that any personal emails are to be short and not frequently sent or received. You are advised that the personal use of the email system is a privilege that you are trusted to use reasonably. However, you should be aware that this privilege may be withdrawn at any time by the principal.

Style

Consideration must always be given as to whether email is an appropriate means of communication in the particular business context. Email is an informal means of communication. Nonetheless, messages sent by email should be written as professionally as a letter or fax. Messages should be concise and directed only to those with a need to receive the communication. General messages to a wide group of people should only be used where necessary.

Confidential Information

Confidential information should only be sent externally by email with the express permission of the principal or where the message has been encrypted.

Email usage during office hours

Best practice for email usage is during school opening hours (7.30 am – 6.00 pm) for both internal and external communication. If composed outside of these hours, please automatically schedule them to be sent during these hours or save to drafts and send the following day.

Automatic Footer

A footer is automatically added to all external emails as set out below. You may not attempt to moderate or remove this footer.

'This email and any files transmitted with it may contain confidential and/or privileged information. It is intended solely for the people or organisations to whom it is addressed. If you are not the intended recipient, any unauthorised copying, disclosure, distribution or other action relating to it is forbidden. This e-mail does not constitute a legally binding agreement. Views or opinions presented in this email do not necessarily represent those of Caroline Chisholm School. We have taken precautions to minimise the risk of transmitting software viruses but advise you to do your own virus checks. We cannot accept liability for any loss or damage caused by software viruses.'

Out of office

If you will be away from the school for longer than a day, you should activate your 'Out of Office Assistant' on your email account to reflect your absence from Caroline Chisholm School. The following is an example of the text which should be used in the automatic reply:

'I am now away from Caroline Chisholm School until [date] / I am out of [the office] this morning returning this afternoon. Please contact [name] in my absence on [telephone number] or [email address]. Your message [has/has not] been automatically forwarded to a colleague.

Kind regards

[name]

[title]'

6.2 Use of the Internet

Business use

Access to the Internet is also primarily provided for business use. Limited personal use of the Internet is permitted providing that it does not interfere with the performance of your duties. Any use of the Internet may not come within the expressly excluded uses (see 6.2.4) or otherwise breach any of the Caroline Chisholm School's rules, policies or procedures.

Downloading Software

Only software for business use may be downloaded from the Internet. You are encouraged to refer any request for downloading software to your head of faculty rather than downloading it yourself. If you have downloaded software from the Internet yourself, you must ensure that appropriate virus checks are carried out and that its use is approved by your head of faculty. You must ensure that no software copyright licences are breached.

Records

All Internet usage is recorded by the School Firewall e.g., username, sites visited and duration of the browsing session. Accordingly, you should not assume that Internet usage is private.

6.3 Misuse of the Email

The email system and the Internet may not be used for accessing, transmitting or downloading any of the following material or using any of the following facilities. Any such actions will amount to gross misconduct which may result in the summary termination of employment with Caroline Chisholm School.

i. Pornographic material (i.e., writings, pictures, films, video clips of a sexually explicit or arousing nature);
ii. Offensive, obscene or criminal material or material which is liable to cause embarrassment to the Academy, any of its employees or students

iii. Abusive, intimidating, hostile, humiliating or aggressive material or material which constitutes harassment or discrimination on the grounds of sex, marital status, sexual orientation, race, colour, nationality, ethnic or national origin, religion or belief, or disability or, from October 2006, age
iv. False or defamatory statements about any person, firm, company or other organisation
v. Confidential information about the Academy, any of its employees or students
vi. Statements which are likely to create liability (whether criminal or civil) for the sender or the school
vii. Material which has been obtained in breach of copyright
viii. Online gambling
ix. Chain letters

6.4 Legal Action against Caroline Chisholm School/or you

Sending an email internally or externally and entering and/or submitting information onto a website is clearly "publication". This means that emails can give rise to legal action against Caroline Chisholm School and against you personally. For example, claims of discrimination, harassment, defamation, breach of confidentiality or breach of contract could result from a misuse of the email or internet system. Emails are potentially disclosable in legal proceedings against you or against the school. Misuse of the Internet can, in certain circumstances, constitute a criminal offence.

6.5 Receipt of Messages

If you receive a wrongly addressed email, you should immediately notify the sender of that email but should not otherwise use or deal with that email except to delete it from your system.

Caroline Chisholm School monitors emails as set out below. One of the purposes of this monitoring is to avoid, wherever possible, employees of the school receiving offensive material. However, it is impossible to ensure that all such material does not reach you. If you receive an email which you find offensive, you should not delete it, but you should ensure that it is not forwarded to any other email address, whether internal or external nor is it printed or copied. It should be reported immediately to your head of faculty, and once instructed by your head of faculty; it should be deleted from your email folder completely.

If you receive an email which you do not find offensive, but which contains material which others may find offensive (in any form, e.g., text, pictures, moving clips, animations or programmes), you must also ensure that it is not forwarded either internally or externally, printed or copied. If such emails are sent internally or externally, they may cause offence to the recipient, harm the school's reputation, and create legal liabilities for the school and for you personally. In this context, the term "offensive material" includes but is not limited to abusive language, pornographic/nude imagery, distressing scenes, and any other information liable to cause offence or depict or contain material which may be considered harassment or discrimination.

6.6 Viruses

Most viruses are transmitted via external emails, and in particular those with attached files. The school's firewall offers some protection, but it is clearly impossible to predict all potential viruses. If you are at all unsure about the attachments that you have received or you think the source of an email is questionable, you should not open them and contact your head of faculty immediately. The school does accept that there is some risk that legitimate business emails may contain a virus. However, the school does not accept the risk of a non-business-related attachment containing a virus. Therefore, you should not open any attachment from an external source that is not connected with the school's business, i.e., personal emails.

6.7 Security

You are responsible for the security of your computer. You must keep your personal passwords confidential and change them regularly. When you leave your terminal unattended or leave the office, you should apply the screen lock or log off the system to prevent unauthorised users from using your terminal in your absence. You must not

allow your terminal to be used by an unauthorised person. In particular, you must ensure that students at the school do not have access to your computer.

You should respect the confidentiality of other employees' emails and should not access or read other employees' emails except where express consent has been given or such action has been duly sanctioned by the head of faculty, where that sanction is reasonable in all the circumstances.

You may not send internal or external emails other than from your own email account.

6.8 Monitoring

Caroline Chisholm School accepts that you have the right to some privacy in the workplace. However, the school reserves the right to check all incoming, outgoing and internal emails and Internet usage if necessary.

Emails may be manually checked for the following purposes:

- to ensure compliance with the school's email and Internet policy
- to investigate suspected abuse of the school's email or Internet, such as accessing pornographic material, sending abusive or insulting emails
- to comply with any legal obligation
- to retrieve data at the user's or a manager's request following a system failure
- to assist with business continuity

The school also blocks access to Internet sites which are unlikely to need to be visited for work-related reasons.

6.9 Data Protection

Caroline Chisholm School and its employees have a legal obligation to protect the data it holds. Staff are expected to abide by the following:

Laptops/Surface Go's/Paperwork are a doorway to our systems and staff and student data. They should rarely if ever, be left unattended, whether in a workroom, classroom or public space.

- Surface Gos and laptops should only be left, if they are left anywhere, in a locked cupboard or drawer
- Workrooms should be left locked if there in no-one in them
- PC/laptop screens should have the screen locked if the machine is being left on
- Students should not be given keys to access workrooms
- There should never be any personal data on the local hard drive of school-issued laptops
- Surface Gos /laptops/paperwork should be kept in the safest place possible
- Surface Gos /laptops must be password/pin protected at all times
- Personal mobile phones should be password/pin protected if used to check work emails
- Password/pin should not be shared
- If there is a suspicion that a password/pin has been compromised, then it should be changed immediately
- Different passwords must be used for SIMS and Office 365 logon
- Password protected documents should also have different passwords to those used for SIMS and Office 365 logon