Salesian College

Assistive Technology Acceptable Use Policy

15-04-2024

Table of Contents

1. INTRODUCTION AND RATIONALE

The following policy aims to maintain a safe, nurturing environment where the personal dignity and rights of all the members of the school community are preserved. The school's policy on Acceptable usage and ICT is therefore devised with the intention of ensuring that teaching and learning can take place without interruption and also with the intention of protecting students and staff from potential harassment or bullying.

Legislation and School Policy

- Education Act 1998
- Health and Welfare at Work ACT 2005
- Child Trafficking and Pornography Act 1998
- Interception of Postal Packet.
- Code of Professional Conduct Teaching Council
- ESPEN ACT 2000
- Child Protection Policy
- Dignity in the Workplace
- Anti-Bullying Policy
- Data Protection Policy
- Code of Behaviour
- Mobile Phone Policy

Scope

- All users of ICT resources both on and off site, within and outside normal working hours
- It applies to all communications regarding Salesian College and IT users within and outside normal working hours
- Salesian College endeavours to ensure that ICT resources are in place to meet the communication, administration, pedagogical and learning and teaching needs of the College. Resources include hardware, software, user accounts, social, local and wide area network facilities as well as services accessed via internet
- Salesian College requires appropriate use of technology and the college right to log and monitor activities such as email content, sites and what is downloaded.
- Each user is responsible for full awareness of ICT policy and its implication for personal conduct
- As in all work and school activities users are required to use ICT resources in a reasonable professional, ethical and lawful manner

POLICY STATEMENT

Aims of the Policy

- Protect and maintain integrity of ICT resources and make communication reliable
- Support teaching and learning
- Implement best practice in the appropriate use of ICT resources
- Implement best practice in the appropriate use of ICT resources
- Ensure uses engage only in the appropriate is of ICT resources to meet needs of students

General Principles

The acceptable use of the school's ICT resources is based on the following principles:

- All ICT resources and related information remain the property of the school.
- Users must ensure that they always use ICT resources in a manner which is lawful, ethical, and efficient.
- Users must respect the ICT devices and equipment provided for their use and take all reasonable steps to prevent damage, loss, or misplacement.
- Users must respect the rights and property of others, including privacy, confidentiality, and intellectual property.
- Users must respect the integrity and security of the school's ICT resources. Breaches of this policy are a matter for the Board of Management to be treated as a matter for discipline. Depending on the seriousness of the breach this will be dealt with by the principal in accordance with the School's Code of Behaviour. For breaches which do not warrant such action, those involved will be advised of the issue and given a reasonable opportunity to put it right.

3. RESPONSIBILITY

Our entire school community have a role in implementing the Policy.

Board of Management

- The Board of Management will approve the policy and ensure its development and evaluation.
- As new technologies are developed that may prove valuable to our teaching and learning goals, to evaluate and provide access to them if necessary.
- To consider reports from the Principal and the ICT Department on the implementation of the ICT policy.

Principal

- The Senior Leadership Team will be responsible for the dissemination of this policy.
- To oversee implementation of the policy.
- To establish structures and procedures for the implementation of the
- To provide all staff, students, parents supply staff, and administrative staff with the school's Policy.
- To notify all parties when the policy has been updated.
- To provide training for staff and students in the appropriate and responsible use of ICT Resources.
- To ensure that users understand that failure to adhere to this Policy will result in the loss of privilege and/or disciplinary action.
- To monitor the implementation of ICT Policy.

ICT Department

The ICT Department consists up of Principal, 2 Deputy Principals ICT Digital Committee.

The ICT Department will coordinate and support the technical implementation of the policy with staff on an ongoing basis.

Responsibilities include:

- Provide input on the implementation of the policy.
- Establish practices and procedures for the implementation of ICT Policy.
- Maintain a list of "Approved ICT Resources".
- Where the policy has been breached, report the breach to the principal.
- Monitor the implementation of the policy and provide feedback to the principal where relevant.
- Only access administrator accounts via their school supplied trusted device.

Non-Teaching Staff

Non-teaching Staff are required:

- To accept the terms of this ICT Policy before using any ICT Resource in the school.
- To monitor their use of ICT resources in line with this policy.
- To immediately report any violation of this ICT Policy as per policy procedure

Teaching Staff

Teaching Staff are required:

- To accept the terms of this ICT Policy before using any IT Resources in the school.
- To instruct and monitors students in their appropriate use of ICT resources as set out in this ICT Policy
- To record any violations of the Policy and inform the Senior Leadership Team.
- To report incidents of online bullying and be mindful of the obligations under Child Protection Guidelines.

Administration Staff

Administration Staff are required:

- To accept the terms of the Policy before using any ICT Resource in the school.
- To monitor their use of ICT resources in line with this policy.
- To immediately report any violation of the Policy to the ICT Department/ SLT.

Students

Students are required:

- To agree to exhibit responsible behaviour in the use of all ICT resources as set out in this ICT Policy
- To accept that the use of personal devices such mobile phones, smart watches, smart phones, smart glasses (any device with connectivity) are prohibited in Salesian Celbridge.
- To accept that the use of Artificial Intelligence e.g. ChatGPT for the completion of homework, projects, course work for state exams is not permitted. (this list is not exhaustive)
- To take personal responsibility for not accessing inappropriate material on the internet.
- To accept that Salesian College Celbridge is not responsible for materials, or information of any kind, placed on the network by third parties.
- Internet sessions will be supervised by a teacher,
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' Internet usage.
- The use of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- Student use of external digital storage media (e.g. Cloud storage, memory sticks/cards, personal USBs, CDROMs etc.) in school requires a teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

- Students are forbidden from opening apps in class or going online, unless instructed to do so, and only for the purposes instructed by a teacher.
- Students will not use school supplied ICT resources for personal reasons.
- School email accounts should not be used to sign up to other non-educational apps or websites.
- Students will use school supplied school email accounts for communications with teachers (using the teacher's school email account).
- Students will not send any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses, telephone/mobile phone numbers or pictures.

Parents / Guardians

Parents/guardians are required:

- To support the school's ICT Policy.
- To become familiar with the school's ICT Policy and to discuss it with their child.
- To accept responsibility for supervision, when a student's use of email and the internet is not in a school setting.

4. THE CHILD TRAFFICKING AND PORNOGRAPHY ACT 1998

The sharing or storing of explicit images is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.

- Every student and staff member in the school always has a right to a safe learning environment in school, free from risk of exploitation.
- The school has a duty of care to students and staff under various legislation including but not limited to the Safety, Health & Welfare at Work Act 2005 as well as the Child Trafficking and Pornography Act 1998 and any other related legislation.
- The Board of Management reserve the right to contact An Gardai Síochána should there be a strong suspicion of a member of staff or student acting illegally using school ICT Resources.

5. MONITORING

The school reserves the right to routinely monitor, log, audit and record all use of its ICT resources for purposes including but not limited to:

- Helping to trace and resolve technical faults.
- Protecting and maintaining network and system security.
- Maintaining system performance and availability.
- Ensuring the privacy and integrity of information stored on the network.
- Investigating actual and suspected security incidents.
- Preventing, detecting, and minimising inappropriate use.
- Protecting the rights and property of the school, its staff, students and wider school community.
- Ensuring compliance with other school policies, current legislation and applicable regulations.

Whilst the school does not routinely monitor an individual's use of its ICT resources it reserves the right to do so when a breach of its policies or illegal activity is suspected. The monitoring may include, but will not be limited to individual login sessions, details of information management systems and records accessed, contents of hard disks, internet sites visited, time spent on the internet, and the content of electronic communications.

Salesian College will always seek to act in a fair manner and respect the individual user's right for the privacy of their personal information under the Data Protection Act 2018. Information collected through monitoring will not be used for purposes other than those for which the monitoring was introduced, unless it is clearly in the users' interest to do so or it reveals activity that the school could not be reasonably expected to ignore, for example a user found to be viewing,
Individual monitoring reports will only be accessible to the appropriate authorised personnel and will be deleted when they are no longer required.

6. ICT DEVICES AND EQUIPMENT

- Purchases of ICT equipment and resources must be vetted through the principal
- ICT resources must be vetted through prior to purchase, subscription, licencing of these ICT resources.
- A record of decisions will also be maintained to demonstrate which ICT resources were approved (or not).
- All ICT devices and equipment provided to staff remain the property of the school.
- ICT devices and equipment will be registered on an Asset Register.
- They will maintain a list of "Approved ICT Resources".
- ICT Devices will be provisioned with appropriate technical measures to safeguard personal data i.e. encryption of hard drives.
- School supplied ICT devices are then known as "trusted devices".
- Staff and students must not remove or borrow school ICT devices or equipment without the authorisation of the BOM
- The security of any school ICT devices and equipment borrowed is the responsibility of the borrower and the ICT devices and equipment must be returned by the borrower.
- Shared devices for student use (Classroom Windows Laptops) will not be configured with a password. Class teachers are responsible for instructing students to log out of their device at the end of class.
- Staff and students must not alter the hardware or software configuration of any school ICT device or equipment without the prior authorisation of the ICT Dept.
- Staff and students must take due care when using school ICT devices and equipment and take reasonable steps to ensure that no damage is caused to the ICT device or equipment.
- Staff and students are not permitted to consume food or liquids whilst using ICT devices or equipment.
- Staff and students must report all damaged, lost or stolen school ICT devices and equipment to the Deputy Principal
- ICT equipment must be returned by staff before they leave the employment of the school.

- Staff and students must notify, 6th year students this will happen automatically, the ICT Department of intentions to leave Salesian College Celbridge and ICT access with be disabled upon leaving including access to Office 365access.
- The school reserves the right to remove any ICT devices and equipment from the network at any time, for reasons including but not limited to:

    1) noncompliance with school policies,
    2) the ICT device or equipment does not meet approved specification and standard, or
    3) the ICT device or equipment is deemed to be interfering with the operation of the network.

    - The school reserves the right to alter, modify or reconfigure any ICT devices i.e. Updates or removal of software at any time.

Old and obsolete school ICT devices and equipment will be recycled in accordance with the requirements of the European Waste Electrical and Electronic Equipment (WEEE) Directive. Staff must notify the ICT Department of old and obsolete ICT devices and equipment and the ICT Department will facilitate the collection and disposal of the devices and equipment.

Mobile Devices

- Staff and students must ensure that school supplied trusted mobile devices provided are always protected.
- Staff and students must take all reasonable steps to ensure that no damage is caused to the device and that the device is protected against loss or theft.
- School devices will only be issued to staff who have signed, acknowledged and accepted of the Policy.
- All school devices are registered with the ICT Department routed through the school network infrastructure and managed securely.
- All school supplied trusted devices provided to staff will be set up with a password to gain access.
- Passwords used to access these trusted devices must not be written down on the device or stored with or near the device.
- When traveling by car, trusted mobile devices should be stored securely out of sight when not in use. Staff and students are advised to avoid storing these devices unattended in the boot of a car overnight.
- The use of school smart devices within a car must always be carried out in accordance with the Road Traffic Act 2006.
- When traveling by taxi, bus, train or plane school laptops, mobile computer devices and smart devices should be always kept close to hand. Avoid placing the devices in locations where they could easily be forgotten or left behind (i.e., in overhead racks or boots of taxis).
- When using a trusted mobile device, staff need to take precautions to ensure the information on the device screen cannot be viewed by others. In addition, Staff and students are advised to connect to Wi-Fi networks that are secure i.e., password protected.

- Staff and students must ensure that all trusted mobile devices provided to them are not accessed (including internet access) by persons who are not school staff or students (i.e., friends, family members and others etc).
- The use of personal devices by students, such as phones, smart watches, smart glasses and tablets are prohibited in Salesian college Celbridge. (This list is not exhaustive)
- Students on admission to Salesian College Celbridge agree to adhere to the school ICT Policy

7. ALLOCATION OF TECHNOLOGY

Assistive Technology

- When a student has received a formal report with a recommendation for Assistive technology, details must be provided to Salesian College stating the recommendation. i.e. psychological reports, Occupational therapy report etc.
- Prior to entering Salesian College, incoming students must provide details of previous school use, and submit formal reports stating Assistive Technology recommendation on completion of school acceptance form.
- Students must adhere to appropriate use as contained in this policy. Any breaches of this will be considered misuse of technology and appropriate sanctions will apply. (Appendix B)
- Parents/guardians must provide information pertaining to the provision of Assistive Technology i.e., purchased by NCSE or personal. (Appendix A1 or A2)
- Where a student has a recommendation for the use of personal devise parents will be responsible for maintaining updates and virus scanning of this devise devices.
- Students must attend school with fully charged devices and bring their own chargers.
- In some cases, a professional report recommends that ICT is to be provided, it is treated it as a recommendation to the school on behalf of the candidate. Such recommendations do not automatically confer eligibility for support or automatic right to use same in examinations. (Appendix B)
- Students will receive allocation of ICT usage in Salesian College Celbridge, provided they meet all eligibility criteria as set out in Reasonable Accommodations for State Exams and Salesian College AEN policy before ICT can be approved.
- Such recommendations do not automatically confer eligibility for support or automatic right to use same in examinations.
- NCSE guidelines will be implemented should issues arise with NCSE purchased assistive technology. These will be dealt with on a case-by-case basis

RACE

The SEC recognises the role of assistive technology in enabling independent access to the examinations by students who are eligible for RACE. The SEC encourages use of available assistive technology to support independent access. The range of assistive technologies which candidates can apply to use under the scheme are:

- Access to a word processor, laptop, or tablet.
- Access to a recording device.
- Access to an exam reading pen* as an alternative accommodation to a reader/ reading assistant for candidates eligible.

Schools do not have delegated authority to recommend any accommodations not listed among the range of available accommodations.

Should a student choose not to use their Assistive Technology, as recommended in their report, Parents/guardians will be informed and encouraged to discuss the implications of this with their son. A letter will be communicated by the AEN to ascertain and acknowledge the parents' guardians'/decision on Assistive technology usage. (Appendix C)

8. HOME USE OF ASSISTIVE TECHNOLOGY

Online Teaching and Learning

School business is normally conducted in person within the school building. In exceptional circumstances and at the discretion of the Board of Management, remote working / teaching / learning may be facilitated only for whole school closures.

Staff who are authorised by the Board of Management to work from home must take all reasonable measures to ensure that access to school ICT Resources including devices and software applications is kept secure and protected against unauthorised access, damage and / or loss.

- All work carried out by Staff on behalf of the school while working at home is done using approved software as per the "Approved ICT Resources List" held with the ICT Coordinator.
- No other platform which is their personal property, or the personal property of another household member should be used – the only exception to this is the ICT Department supporting persons using school domain accounts in the normal course of delivering services to the school.
- School devices must not be used by family members or other persons.
- Passwords to school devices must be kept confidential and must not be shared with family members or third parties.
- In the event that such a device is lost or stolen, or is suspected of having been lost or stolen, the SLT / ICT Department must be informed as soon as possible so that such steps as may be appropriate may to mitigate the consequences of the loss.

- All school supplied trusted software used by staff and students to work from home should be password protected in accordance with this policy.
- All confidential and restricted information which is accessed by them must be always kept secure and confidential.
- All school software and information provided to them are not accessed (including internet access) by members of their family, other household members or visitors.

Protocol for Remote Learning & Live Classes

Each teacher and student have been assigned an individual account, username and password for Microsoft Office for Education which they can use for remote teaching and learning.

- Only the individual to whom the account was assigned is permitted to use such account i.e. Each school account is for the sole use of the teacher / student only.
- The school will only correspond with the account holder, and should there be a breach of this policy, the school will suspend the account indefinitely.
- Only teachers are permitted to record live classes.
- Students are expected to conduct themselves with respect for both the teacher and their classmates

Protocol for Live Meetings

Should the school need to revert to online meetings for both staff and student meetings.
Each teacher and student have been assigned an individual account, username and password for Microsoft Office which they can use for remote teaching and learning.

- Online Meetings where held i.e. Subject Department meetings, meetings with the Senior Management, Staff Meetings are permitted to take place on conferencing software as identified on the "Approved ICT Resources" list held with the Deputy Principal
- Only the individual to whom the account was assigned is permitted to use such account i.e. Each school account is for the sole use of the teacher or student.
- Staff should consider all meetings on conferencing software as potentially sensitive and ensure that they are in a quiet room where others cannot overhear the discussion.
- The use of WhatsApp is not permitted for communications involving personal data.
- Staff and students should exercise due care when live messaging / emailing during class i.e. ensure that the intended recipient(s) is being communicated with.
- The sharing of personal data should be limited to only those (i.e. staff) who need to know.
- Staff must take appropriate measures to secure data i.e. password protect any documents containing personal data and send this information only to those who need it via email.
- Minutes of meetings should be saved to the school's cloud and never locally to a personal storage device.

When teachers are conducting one to one session with students i.e. regarding Counselling, SEN, Disciplinary matters. The following protocol applies:

- School supplied conferencing software should be used to set up and conduct the meeting.
- Video may be used and, at either party's discretion may be turned off.
- The meeting shall not be recorded.
- If a student abruptly ends the meeting, the staff member is required to prepare a short report detailing the topic of discussion, matters raised etc. This report must be sent to the Principal and / or Deputy Principals within 24 hours of the meeting taking place.

- Where staff take notes, it is their responsibility to keep this data safe and secure.
- Where actions / next steps are agreed, they should be recorded and stored secure.

SOCIAL MEDIA

Social Media Accounts

- Staff and students are not permitted to setup Social Media Accounts on behalf of / posing as Salesian College without the expressed written permission of the principal.
  There is a designated member of staff with access to all Social Media Platforms whose responsibility is to upload content to the above platforms. All uploaded content will have prior approval from the principal.
- The use of personal social media accounts e.g, WhatsApp, text, (this list is not exhaustive), is not permitted for any school communications.
- All school communication must take place using formal means. I.e. School phone, email.
- The Code of Professional Conduct published by the Teaching Council governs the use of Social Media sites by teaching staff.
- Non-teaching staff are expected to exercise sound judgement and maintain the highest professional standards while using social media in the school.
- All staff are encouraged to use the privacy settings on social media sites/apps and to keep updated on developments on privacy restrictions

Software & Electronic Media

Each member of staff is responsible for making use of software and electronic media in accordance with the Irish Copyright and Related Rights Act 2000 and software licensing agreements. An "Approved ICT Resources" List is maintained by the Staff should consult the Principal and ICT Department before purchasing downloading, accessing or using any 3rd party software in connection with school business.

- Only software which has the correct and proper licence may be installed and used within the school.
- Software and mobile apps must only be downloaded and installed on school supplied trusted devices where there is a valid school reason, and the software can add value to teaching and learning in the school.
- All software and electronic media developed and purchased on behalf the school remains the property of the school and must not be used, copied, distributed or borrowed without the authorisation of the principal
- The school reserves the right to remove software at any time, for reasons including but not limited to:
- Non-compliance with school policies
- The software is not properly licenced.
- The software is found to have a negative impact on the performance of the school network, systems or equipment.

MICROSOFT TEAMS

The Management Information System, Microsoft 365 have been provided for teaching and learning in Salesian College When using a personal (non-school supplied device) to access these ICT Resources the following applies:

- Access is restricted to the browser i.e. staff are not permitted to download related apps. Accessing email (as an example) must be done through the browser only. Login details for these systems must not be saved / cached in the browser. In addition, staff are not permitted to download or store school related personal data to their personal device.
- Such devices must be secured by a password.
- Passwords should be sufficiently memorable that the user can avoid writing them down, but not obvious or easily guessed.
- Such devices must be configured so that they are automatically locked after being left idle for a set time e.g., 1 minute.
- Such devices must not be used by family members or other persons. Passwords to such devices must be kept confidential and must not be shared with family members or third parties.
- Care must be taken to avoid using such devices in a manner which could pose a risk to confidentiality, or personal data whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using wi-fi facilities in public places (e.g., coffee shops or airports), or otherwise.
- In the event that such a device is lost or stolen, or is suspected of having been lost or stolen, the principal must be informed as soon as possible so that such steps as may be appropriate may be taken to mitigate the consequences of the loss.
- Home Wi-Fi networks must be encrypted. Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure. o If such a device needs to be repaired, appropriate steps must be taken to ensure that confidential information or personal data cannot be seen or copied by the repairer.
- In the event that such a device needs to be disposed of, confidential material must be destroyed or wiped using a recognised method to put the data beyond recovery, to the satisfaction of Salesian College.
- In order to protect the information that is accessible on Management Information System, users must not divulge their logon details to third parties.
- Any concerns or queries must be forwarded and dealt by an Administrator with rights on the Management Information System, Microsoft 365
- Staff must ensure they have strong passwords associated with their accounts i.e. a minimum of 8-12 characters with a mixture of upper case, lower case, number and symbols.

Passwords

Where appropriate individual users will be granted access to the school's ICT resources which are necessary for them to perform a specific task in the school.

Each authorised user will be assigned an individual user access account name and password set which they can use to access a particular ICT resource.

Accounts will be provisioned on a "least privileged access" basis i.e., a user is given the minimum levels of access, or permissions needed to perform his/her function.

Staff and students are not permitted to access the school accounts of others.

Should a member of staff or student access a school device and finds another member of staff/student has not logged out, the person accessing the device must log the other person out before proceeding to use the device.

Each user is responsible for all activities performed on any ICT device, management information system or software application while logged in under their own individual access account and password.

Staff and students must ensure all passwords assigned to them are kept secure.

Staff and students should not use the same password for their personal accounts i.e. social media as their school supplied accounts.

Staff and students who suspect their password is known by others must change their password immediately.

Staff and students must ensure all default passwords which are supplied by a provider are changed in line with this policy as soon as could be reasonably.

EMAIL – OUTLOOK

Staff and students are encouraged to send email correspondence during normal working hours i.e. 0830 to 1700 Monday to Friday.

Staff and students may also consider scheduling emails to be sent during these times if they wish i.e. scheduling an email to be delivered at 0830 the following morning.

Teachers and students are advised that they are under no obligation to respond to emails outside normal working hours.

- Teachers will use trusted school supplied email accounts for all communications.
- Teacher's use of email is facilitated strictly in an educational context and access to personal email and/or social networking accounts is prohibited.
- Staff and students must not send any emails that are likely to cause distress or any material which is offensive, indecent, obscene, menacing, or in any way unlawful.
- The school network must not be used to send or distribute unsolicited commercial mail, commonly known as 'spam', in bulk or individually.
- Where emails and attachments contain sensitive personal information, staff are required to password protect attachments to these emails. Attachments including sensitive personal information should be password protected i.e. ensuring only the recipient(s) with a password can open and access the contents of the email.
- Staff and student should not save copies of personal data to school computers, phones, tablets, USB sticks, Hard Drive

Confidentiality & Privacy

The school as a Data Controller is legally required under the Data Protection Act 2018 to ensure the security and confidentiality of all personal data it processes.

- Staff and students must respect the privacy and confidentiality of personal data at all times.
- Staff must not access personal data or management information systems unless they have a valid school related reason to do so, or they have been granted permission by Senior Management
- Staff must not remove any confidential or restricted personal data (irrespective of format) from the school without the authorisation of the principal.
- Confidential and restricted personal data must only be discussed or shared with others on a strict "need to know" basis.
- Confidential and restricted personal data must only be discussed or shared with other staff or staff of a government funded agency in accordance with the school's Data Protection Policy.
- Confidential and restricted personal data must only be released / disclosed to other government agencies and departments in accordance with the relevant legislation where there is a valid written request.
- Where it is necessary to release or disclose confidential or restricted personal data to third parties, only the minimum amount of data should be released as is absolutely necessary for a given function to be carried out.
- Appropriate technical & organizational measures should be adopted to ensure that data is kept secure i.e. password protecting documents before emailing. • Confidential or restricted personal data (irrespective of the format) must not be copied, renamed, deleted or modified without the authorisation of the principal. This includes personal data on storage devices and information in transit.
- Personal data belonging to school staff or students must not be used for presentations, training or testing purposes unless it has first been anonymised or pseudonymised (coded). Otherwise, the explicit consent of the school and the individual (as a Data Subject) is required from the parent / guardian of the student (where students are under 18 years).
- Staff must ensure that all software applications or network access provided to them are not accessed (including internet access) by persons who are not school Staff (i.e. friends, family members and others etc). Please refer to the school's Data Protection Policy which provides clear guidance regarding the expected use of personal data in the school. The policy is available from the principal.

REPORTING ON INAPPROPRIATE CONTENT

- The teacher receives the information and with Year Head/ DP or DLP as appropriate receives report of child protection concern.
- DLP records the report-date/time/context.
- DLP makes the decision on how to proceed based on information received.
- Implement Child protection Policy report if required

MISUSE OF PERSONAL DEVICES AND SANCTIONS

Including Mobile phones, Smart watches, Smart phones ipads (this list is not exhaustive)
Misuse of personal devices will be implemented as per code of behaviour as stated below.

The use of mobile phones has caused significant disruption, and stress, to teachers, in recent years.

- Calls being made to students when they are in class and texting in class are some of the difficulties. Consequently, the school has put the following directive in place:
- The use of mobile phones is not permitted between 8.30am and 6.15 p.m. (Following afterschool study). All mobile phones must be turned off in school. The following can

constitute use of a mobile phone on the school premises: accessing the phone in any way for information, check the time, calendar, text messages, taking photographs, making a recording (video, voice, making a note), using any apps or other mobile phone functions.

- Breach of this rule will result in immediate confiscation of the phone for the rest of the day.
- The phone will be returned at the day and a sanction of either a €45 fine or 1 day suspension will be imposed.
- Students will have five days to arrange payment of this fine through the school Easypayments on-line electronic payment system. If the fine is not paid within this five-day limit, a suspension will automatically be applied.
  Camera phones potentially present very serious harassment, bullying and issues of privacy.
- The Board of Management is charged with the duty to protect all members of the school community.

The directive the Board has put in place is as follows:

- There is a complete ban on the use of camera phones.
- Any person found using such a phone faces an automatic one-day suspension or a €45 penalty where it is a first offence.
- The term 'using' includes the activities of either sending or receiving messages, accessing digital content, or accessing information on the phone.
- Second and subsequent offences will result in an automatic one-day suspension.
  Audio/Camera/video recording This use of audio/camera or video recording functions of these devices is not permitted at any time while in the college, on the college grounds or when students are travelling to or from the school. This also applies to school trips and extra-curricular activities. Any inappropriate use of audio, camera or video recordings during school time or activities will result in a serious sanction, which may include suspension.
- At Saleisan College students must not take, use, share, publish or distribute images of others without expressed permission from staff.
- Talking photographs or videos on school grounds or when participating in school activities is only allowed with expressed permission from staff.
- Care should be taken when taking photographic or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

MISUSE OF DIGITAL TECHNOLOGIES AND SANCTIONS

The following list should not be seen as exhaustive. The school has the final decision on deciding what constitutes unacceptable use. The school will refer any use of its ICT resources for illegal activities to the Gardai.

- Excessive personal use.
- Commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit.
- Political activities, such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions.
- To knowingly misrepresent the school.
- To transmit confidential or restricted information outside the school unless the activity has been authorised by the principal.
- To store or transfer confidential or restricted information on a USB memory stick.
- To enter into contractual agreements inappropriately i.e. without authorisation.

- To create, view, download, host or transmit material (other than staff who are authorised by the school to access such material for research etc.) of a pornographic or sexual nature or which may generally be considered offensive or obscene and could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs. material is defined as information (irrespective of format), images, video clips, audio recordings etc.
- To retrieve, create, host, or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others.
- To retrieve, create, host, or transmit material which is defamatory.
- To use Artificial Intelligence site such as CHATGPT (this list is not exhaustive) to complete homework, projects or State Examinations prescribed Coursework.
- Any activity that would infringe intellectual property rights (e.g. unlicenced installation, distribution or copying of copyrighted material).
- For any activity that would compromise the privacy of others.
- For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to the school or others.
- Any activity that would deliberately cause the corruption or destruction of data belonging to the school or others.
- Any activity that would intentionally waste the school's resources (e.g. staff time and ICT resources). Any activity that would intentionally compromise the security of the school's ICT resources, including the confidentiality and integrity of information and availability of ICT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection).
- The installation and use of software or hardware which could be used to probe or hack the school ICT security controls.
- To install and use of software or hardware which could be used for the unauthorised monitoring of electronic communications within the school or elsewhere.
- To gain access to information management systems or information belonging to the school or others which you are not authorised to use.
- Creating or transmitting "junk" or "spam" emails. This includes but is not limited to unsolicited commercial emails, jokes, chain-letters or advertisements.
- Any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.

Unacceptable Uses of Social Media sites and the consequences of that Use

- All members of the school community are responsible for their own behaviour when communicating school related business using social media and will be held accountable for the school related content of their communications that they posted on social media locations.

Examples of Unacceptable Use of Social Media

- Posting of school content on personal social media accounts.
- Sending or posting discriminatory, harassing, negative comments, threatening messages or images that may cause harm to any member of the school community.
- Forwarding, 'Liking' or commenting on school related material that is likely to cause offence or hurt to a third party.
- Sending or posting messages or material that could damage the school's image or a person's reputation.
- Creating a fake profile that impersonates any other member of the school community.

- Sending or posting material that is confidential to the school.
- Participating in the viewing or exchanging of inappropriate images or obscene material.
- Image based sexual abuse. This list is not exhaustive.

While all cases involving the inappropriate use of social media will be dealt with on an individual basis, the school and its Board of Management considers the above to be serious breaches of this policy. Disciplinary action will be taken in the case of inappropriate use of social media tools. For teachers, infringements of this policy will be dealt with in accordance with the Teaching Council Code of Conduct and Disciplinary Procedures. Please note that some inappropriate behaviour may be the subject of mandatory reporting to the relevant authorities or agencies.

The Code of Professional Conduct published by the Teaching Council governs the use of Social Media sites by teaching staff.

- Non-teaching staff are expected to exercise sound judgement and maintain the highest professional standards while using social media in the school.
- All staff are encouraged to use the privacy settings on social media sites/apps and to keep updated on developments on privacy restrictions. Unacceptable Uses of Social Media sites and the consequences of that use
- All members of the school community are responsible for their own behaviour when communicating school related business using social media and will be held accountable for the school related content of their communications that they posted on social media locations. Examples of Unacceptable Use of Social Media
- Posting of school content on personal social media accounts.
- Sending or posting discriminatory, harassing, negative comments, threatening messages or images that may cause harm to any member of the school community.
- Forwarding, 'Liking' or commenting on school related material that is likely to cause offence or hurt to a third party.
- Sending or posting messages or material that could damage the school's image or a person's reputation.
- Creating a fake profile that impersonates any other member of the school community.
- Sending or posting material that is confidential to the school.
- Participating in the viewing or exchanging of inappropriate images or obscene material.
- Image based sexual abuse. This list is not exhaustive. While all cases involving the inappropriate use of social media will be dealt with on an individual basis, the school and its Board of Management considers the above to be serious breaches of this policy. Disciplinary action will be taken in the case of inappropriate use of social media tools. For teachers, infringements of this policy will be dealt with in accordance with the Teaching Council Code of Conduct and Disciplinary Procedures.

Confidentiality & Privacy

The school as a Data Controller is legally required under the Data Protection Act 2018 to ensure the security and confidentiality of all personal data it processes.

- Staff must respect the privacy and confidentiality of personal data at all times.
- Staff must not access personal data or management information systems unless they have a valid school related reason to do so, or they have been granted permission by Senior Management and / or the ICT Department.

- Staff must not remove any confidential or restricted personal data (irrespective of format) from the school without the authorisation of the principal.
- Confidential and restricted personal data must only be discussed or shared with others on a strict “need to know” basis.
- Confidential and restricted personal data must only be discussed or shared with other staff or staff of a government funded agency in accordance with the school’s Data Protection Policy.
- Confidential and restricted personal data must only be released / disclosed to other government agencies and departments in accordance with the relevant legislation where there is a valid written request.
- Where it is necessary to release or disclose confidential or restricted personal data to third parties, only the minimum amount of data should be released as is absolutely necessary for a given function to be carried out.
- Appropriate technical & organizational measures should be adopted to ensure that data is kept secure i.e. password protecting documents before emailing.
- Confidential or restricted personal data (irrespective of the format) must not be copied, renamed, deleted or modified without the authorisation of the Principal. This includes personal data on storage devices and information in transit.
- Personal data belonging to school staff or students must not be used for presentations, training or testing purposes unless it has first been anonymised or pseudonymised (coded). Otherwise, the explicit consent of the school and the individual (as a Data Subject) is required from the parent / guardian of the student (where students are under 18 years).
- Staff must ensure that all software applications or network access provided to them are not accessed (including internet access) by persons who are not school Staff (i.e. friends, family members and others etc).

This policy was formally ratified by the Board of Management on 15th April 2024.

SALESIAN COLLEGE

"We care, develop and believe - together we achieve."

Appendix A 1

Use of personal laptop in Salesian College

Student Name	
Laptop Make/Brand	
Serial Number	

I confirm that I accept responsibility for my sons's use of his personal laptop in school. I understand that I am responsible for any damage that may be incurred and I confirm that I have read, fully understand and accept the Terms and Conditions attached to this policy and agreement and other relevant policies as are determined by Salesian College, Celbridge, Co.Kildare.

Signature of Student		
Student's year when this agreement was signed		
Name of Parent/Guardian (Block Capitals)		
Signature of Parent/Guardian		
Date		
Address		
Contact Numbers	Mobile	Home
Email Address		
Signature of Principal		
Date		

SALESIAN COLLEGE
"We care, develop and believe - together we achieve."

Appendix A2

Use of NCSE allocated Assistive Technology in Salesian College

Student Name	
Laptop Make/Brand	
Serial Number	
Value of laptop	
List of accompanying equipment (e.g headphones, microphone etc.) Please describe each item	
Value of accompanying equipment	

I confirm that I accept responsibility for taking into my possession a laptop/tablet and or other device which will remain the property of Salesian College, Celbridge, Co. Kildare. Roll Number 61661P. These must be returned to the school at holidays and on completion of my son's education in Salesian College.

I confirm that I accept responsibility for my son's use of NCSE laptop in school and I confirm that I have read, fully understand and accept the Terms and Conditions attached to this policy and agreement and other relevant policies as are determined by Salesian College, Celbridge, Co. Kildare.

Signature of Student		
Student's year when this agreement was signed		
Name of Parent/Guardian (Block Capitals)		
Signature of Parent/Guardian		
Date		
Address		
Contact Numbers	Mobile	Home
Email Address		

Signatu	

SALESIAN COLLEGE

"We care, develop and believe - together we achieve."

Appendix A2

Use of NCSE allocated Assistive Technolgy in Salesian College

Student Name	
Laptop Make/Brand	
Serial Number	
Value of laptop	
List of accompanying equipment (e.g headphones, microphone etc.) Please describe each item	
Value of accompanying equipment	

I confirm that I accept responsibility for taking into my possession a laptop/tablet and or other device which will remain the property of Salesian College, Celbridge, Co. Kildare. Roll Number 61661P. These must be returned to the school at holidays and on completion of my son's education in Salesian College.

I confirm that I accept responsibility for my son's use of NCSE laptop in school and I confirm that I have read, fully understand and accept the Terms and Conditions attached to this policy and agreement and other relevant policies as are determined by Salesian College, Celbridge, Co. Kildare.

Signature of Student		
Student's year when this agreement was signed		
Name of Parent/Guardian (Block Capitals)		
Signature of Parent/Guardian		
Date		
Address		
Contact Numbers	Mobile	Home
Email Address		

Signature of Principal	Date:

SALESIAN COLLEGE

"We care, develop and believe - together we achieve."

Appendix B

Use of Assistive Technology in Salesian College

I confirm that I have read, fully understand, and accept the Terms and Conditions within this policy in relation to using Assistive Technology in Salesian College.

I understand that students will not be tested for eligibility for reasonable accommodations in the State Examinations until 3rd year & will not have confirmation of ability to use a laptop until April of 3rd year. We cannot guarantee that a laptop can be used for the Examinations.

All students using Assistive Technology must follow our appropriate use section within this policy. If this is not being followed assistive technology will be removed from a student and they will no longer have permission to use it in school.

Signed: _____Parent/Guardian Date: _____

PLEASE SIGN THIS ACKNOWLEDGEMENT AND RETURN IT TO THE SCHOOL

SALESIAN COLLEGE

"We care, develop and believe - together we achieve."

Appendix C

Dear Parent/ Guardian

It has come our attention that your son _____ has not been using the Assistive Technology that has been recommended. I have discussed this issue with him and he is states that he no longer wishes to use this Assistive Technology.

This may affect the results of his exams, state and inhouse.

Please can you discuss this issue with _____ sign return this letter as an acknowledgment of the format he will use to complete all his assignments and exams.

Please feel free to contact me if you wish to discuss this further.

Regards

Gemma Moore & Feena Pender

PLEASE SIGN THIS ACKNOWLEDGEMENT AND RETURN IT TO THE SCHOOL

I received your letter concerning my sons' use of Assistive Technology. I am aware that_____ is not using it. I give my him permission to complete all assignments and exams in handwriting and I understand that this may have implications for State exams.

If you do not complete and return the above form, you have agreed you son will use Assistive Technology for all class work.

Signed: _____Parent/Guardian Date: _____

Maynooth Road
Celbridge
Co. Kildare
W23 W0XK

Tel: +353 1 627 2166 or +353 1 627 2200
www.salesianscelbridge.com
e-mail: office@salesianscelbridge.com
Registered Charity Number: 20012250

Principal: Ms Brenda Kearns
Deputy Principal: Mr Martin Kerins
Deputy Principal: Mr John Leonard
School Roll Number: 61661P

Appendix D

Receipt of NCSE Purchased Equipment

Student Name	
Laptop Make/Brand	
Serial Number	
Value of laptop	
List of accompanying equipment (e.g. headphones, microphone etc.) Please describe each item	
Value of accompanying equipment	
Signature of Parent/Guardian to show that this equipment was received	
Date	
Signature of Teacher	

Maynooth Road
Celbridge
Co. Kildare
W23 W0XK

Tel: +353 1 627 2166 or +353 1 627 2200
www.salesianscelbridge.com
e-mail: office@salesianscelbridge.com
Registered Charity Number: 20012250

Principal: Ms Brenda Kearns
Deputy Principal: Mr Martin Kerins
Deputy Principal: Mr John Leonard
School Roll Number: 61661P