SALESIAN COLLEGE
E SAFETY POLICY

Author	*Assistant Head Academic*
SLT Approved Date	*15 June 2021*
Governors Approved Date	*16 June 2021*
Review schedule	*Triennial*
Date of next review	*June 2024*

CONTENTS

The e-Safety Policy is part of the Staff Handbook and links to other policies given in various sections of the Staff Handbook, as listed below:

2.15 – Use of Internet, DVD and Licences

3.20 – Staying Safe Online

3.22 – iPad Classroom Rules (Student Planner)

9.2 – Safeguarding Children

9.8 – Data Protection Policy

9.8.1 – Personal Data Retention and Erasure Guidelines

9.8.2 – Taking, Storing and Using Images Policy

9.8.9 – Student Data Protection Policy

9.7.1 – iPad Responsible User Policy (Staff)

9.7.2 – iPad Responsible User Policy (Students)

9.7.3 – Internet Acceptance Form for New Students

9.10 – Mobile Phone

INTRODUCTION

At Salesian College, our mission of "Educating for Life" is central to all that we do to inspire high level creativity, critical thinking, collaboration and communication amongst our students, assisting them to excel academically and inspiring life-long learning within the moral framework of a Christian community.

The integration of technology into teaching and learning plays a critical role in achieving our mission and in equipping our students for life in the modern world. Whilst the College is eager to provide all students with the many opportunities that technology can offer in the classroom, we are very aware of the need to protect and educate all members of our community in their use of technology and of our responsibility to have mechanisms in place which enable effective monitoring, intervention and support should any incidents occur.

The College treats all Safeguarding issues seriously and is fully aware of its responsibility to define the parameters within which the community works and to update the community regularly. A robust and comprehensive e-Safety policy is key in helping to ensure that the College meets its broader Safeguarding objectives and also defines acceptable and responsible use of IT by all members of the College community so that they remain safe and legal.

On-line safeguarding or "e-Safety", as with all technological issues, is an area that is evolving constantly and as such, this policy will be reviewed regularly. Its main purposes are:

- to ensure that the whole College community has the knowledge and skills to stay safe when using technology
- to ensure that the College maintains up-to-date knowledge and understanding of potential risks and that these are identified, assessed and mitigated (if possible), thereby reducing any potential risks to members of the College community, the College as an organisation, or the College's IT infrastructure

As evidence of action of our e-Safety policy:

- all members of the College staff are required to sign to indicate that they have received, read and understood all aspects of this policy before they are given access to the College network and systems, as well as further specific policies such as the *Responsible User Policy for iPads (Staff)* before they are provided with an iPad
- all College students are required to sign the *IT User Agreement (Students)* before they are given access to the College network and systems as well as the *Responsible User Policy for iPads (Students)* before they are provided with an iPad

This e-Safety Policy should be read in conjunction with the *Safeguarding Children Policy*.

TECHNOLOGIES COVERED BY THE E-SAFETY POLICY

This policy is designed to cover use of the following technologies by students and staff at Salesian College:

- PCs
- Laptops
- iPads
- mobile phones
- websites
- the College VLE

- e-mail
- instant messaging / texting
- chat rooms
- social media
- subscription services such as *Doddle* and *GCSEPod*
- *Clarion Call*

IMPLEMENTING AND REVIEWING THE POLICY

The original draft of this e-Safety Policy was developed by members of the College's IT Committee, comprising of:

- The Governor with responsibility for IT
- The Assistant Headteacher with responsibility for Digital Learning
- The Head of Computing
- The IT Manager

The draft policy was reviewed and amended by the following groups before implementation:

- The Governors' IT Committee
- The Senior Leadership Team
- The Designated Safeguarding Lead: The Deputy Headteacher
- The IT Support Team

Following implementation, the e-Safety Policy will be:

- Reviewed every three years and/or following any e-Safety incident

ROLES, RESPONSIBILITIES AND ACCOUNTABILITIES

The Governing Body

The Governing Body is accountable for ensuring that this policy is robust and fit for purpose. As such it will review this policy every two years, or following any e-Safety incident, or following any changes to statutory guidance for schools which would affect this policy, thereby ensuring that the policy is up-to-date and applicable with regard to all aspects of technology in use within the College. Review will also ensure that the detail of the policy is effective in dealing with any perceived potential incident or threat.

The Headmaster

Reporting to the Governing Body, the Headmaster holds overall responsibility for e-Safety within the College, but he may delegate some or all of these responsibilities to other named members of staff (*the e-Safety Responsible Persons)* whose roles are defined below.

The Headmaster will ensure that:

- a planned programme of up-to-date e-Safety training and/or awareness raising is in place for all members of the College community (staff, students, governors and parents)
- the designated e-Safety Responsible Persons have received sufficient and appropriate professional development/training, thereby allowing them to discharge their duties effectively
- all e-Safety incidents are dealt with promptly and appropriately

The e-Safety Responsible Persons

The Deputy Headteacher (as Designated Safeguarding Lead) will:

- maintain an overview of e-Safety issues
- act on e-Safety incidents as reported to him and maintain records

The Assistant Headteacher (Pastoral) will:

- ensure that the PSHE curriculum covers e-Safety issues and that e-Safety updates/events are provided annually for parents

The Head of Computing will:

- ensure that the computing curriculum covers e-Safety issues

The IT Manager will:

- ensure that College IT systems are in place, working and up-to-date for the protection of students, staff and the systems themselves

Reporting to the Headmaster, the e-Safety Responsible Persons will, in their areas of responsibility:

- keep up-to-date regarding the risks posed by technology to all users (whether in College or at home), through appropriate research, reading, provision of resources and attendance at accredited training events
- advise the Headmaster and Governing Body on e-Safety matters
- ensure that the e-Safety policy is reviewed every two years, reporting any issues to the Headmaster
- engage with all members of the College community (staff, students, governors and parents) regarding e-Safety matters

- Retain responsibility for the reporting and recording of e-Safety incidents
- liaise with the IT Support Team to ensure that all technical e-Safety measures in College are fit for purpose (e.g. internet filtering software, behaviour management software)
- liaise with the Headmaster and IT Support Team regarding decisions on appropriate staff and student access to internet based resources within College
- plan and ensure the delivery of up-to-date e-Safety training and/or awareness raising is in place for all members of the College community (staff, students, governors and parents)

The IT Manager (and IT Support Team)

- The IT Manager and team are responsible for ensuring that:
- The IT technical infrastructure is secure; this will include as a minimum:
    - anti-virus software that is fit-for-purpose, up to date and applied to all capable devices
    - monitoring software updates and installing updates as appropriate
    - ensuring the correct operation of internet filtering
    - ensuring that filtering levels are applied appropriately and according to the age of the user and that categories of use are discussed and agreed with the e-Safety Responsible Persons and Headmaster
    - ensuring that password protocols are applied correctly to all users
    - the IT System has a secure password and access policy

Teaching and Support Staff

All staff must ensure that:

- all details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headmaster.
- any e-Safety incident must be reported to the Deputy Headteacher (as DSL), or in his absence to the Headmaster. If you are unsure whether or not to report an incident, the matter must be raised with the Deputy Headteacher, or the Headmaster to make a decision
- they sign to indicate that they have received, read and understood all aspects of this policy and associated policies:
    - *Staff use of Social Media*
    - *Responsible User Policy for iPads (Staff)*
    - *Responsible User Policy for iPads (Students)*

Students

e-Safety education is embedded into the curriculum - students will be given appropriate advice and guidance by staff, in all subject areas across the curriculum.

All students must:

- ensure that they are aware of methods by which they can report areas of concern whilst at school or outside of school
- sign to indicate that they have received, read and understood the *IT User Agreement (Students)* before they are given access to the College network and systems and the *Responsible User Policy for iPads (Students)* before they are provided with an iPad

Parents and Carers

Parents have a key responsibility in ensuring that their child uses technology appropriately and safely. The College will:

- ensure that parents are given access to resources to acquire the knowledge they need to ensure the safety of their child outside of the school environment.

It is important that parents understand that the College needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will be asked to countersign any agreement or policy acceptance document that students sign.

TEACHING AND LEARNING ABOUT E-SAFETY

The College has a responsibility to ensure that all students are fully aware of the risks of using all aspects of technology and how to mitigate against these. The College, through the e-Safety Responsible Persons, undertakes to put into place appropriate education and training to assist students in keeping themselves and others safe, secure and legal when using technology and how to mitigate against possible risks through:

- specific e-Safety lessons as part of the PSHE programme
- specific e-Safety lessons as part of the Computing curriculum
- providing access to external speakers and presentations

MANAGING THE SECURITY OF INFORMATION

The security and integrity of the College's information and data is of the upmost importance and is governed by the Salesian College IT Security Policy.

MANAGING DATA STORAGE AND PROCESSING

The College takes its compliance with the Data Protection Act 2018 (DPA 2018) seriously, it being the UK's implementation of the General Data Protection Regulation (GDPR). Personal data will only be recorded, processed, transferred and made available in accordance with this legislation. Full details can be found in the College's *Personal Data Retention and Erasure Guidelines Student* and *Data Protection* policies.

Staff and students are expected to save all data relating to their work to the College's network drives which are backed up daily. Staff may only take information offsite on a password protected device and only when it is necessary and required in order to fulfil their role.

Any security breaches or attempts, loss of equipment and/or any unauthorised use or suspected misuse of IT must be immediately reported to the Deputy Headteacher.

MANAGING PERSONAL INFORMATION RELATING TO STAFF AND STUDENTS

The College contact details as provided on the College website are limited to the school address, reception email address and College telephone number.

A list of staff names and qualifications is given on the web-site, but no other personal information about staff will be given.

The College makes use of images of pupils during their time at the college. The taking, storage and use of images is governed by the *Taking, Storing and Using Images of Children Policy.* Some use is necessary for administration purposes and the safety of pupils, such as CCTV, whilst others such as College media, including photos of pupils at work or playing games, may be included on the College website, College social media feeds, or as part of a College prospectus or magazine. In the publication of pupils' images or work, their full names will not be used, particularly in association with photographs. Written consent from both parents/guardians and the students themselves is obtained before photos of students are published. Parents and students are required to sign the *Use of Images of Pupils by Salesian College* agreement. Non-return of the agreement will be taken to mean that permission has NOT been granted. Where appropriate the College will also seek further consent, for instance before using a student's photo for the purposes of published advertisements.

MANAGING FILTERING

The School takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a College computer. The College cannot accept liability for the material accessed, or any consequences of internet access. The College monitors ICT use carefully to establish if the e-Safety Policy is adequate and to ensure that the implementation of the e-Safety Policy is appropriate and effective.

Any requests for changes to the College's filtering parameters must be made to the IT Manager. A log of all requests is kept

PASSWORD SECURITY

Staff and students are regularly reminded of the need for password security. All students and members of staff must:

- use a strong password
- not write passwords down
- not share passwords with other pupils or staff

MANAGING AND AUTHORISING HARDWARE/INTERNET ACCESS

ACCEPTABLE HARDWARE/SOFTWARE USE

The IT system is owned by the College and may be used by staff and students to enhance teaching, learning administration and management through use of College computers, laptops and iPads, using software provided by the College. The College's e-Safety Policy has been drawn up to protect all parties (i.e. the staff, students and the College) in the use of this system. The College reserves the right to examine or delete any files that may be held on its computer system and to monitor any internet sites visited.

Teaching staff and students are not permitted to attempt to install software on any part of the computer system.

ACCEPTABLE INTERNET USE

Staff requiring internet access are expected to comply with the terms and conditions detailed in the *Internet Acceptable Use Policy.*

Members of staff may place themselves in breach of contract if the above terms are not met.

STUDENTS STAYING SAFE ONLINE

Top Tips for staying safe on line are published in students' planners. Staff should familiarise themselves with these tips and should reinforce them regularly when teaching.

E-MAIL

E-mail communication to and from College e-mail addresses is not private. All e-mail to and from College e-mail addresses is monitored, including monitoring for offensive language. Students must immediately inform a member of staff should they receive an e-mail which includes material which could be regarded as illegal, obscene, racist, violent, threatening, demeaning, or pornographic in nature. Should staff receive such an e-mail, they should immediately inform the Deputy Headteacher and the IT Manager. Students must not share personal details about themselves or others via e-mail communication without specific permission. Communication between staff and students via e-mail must only take place via a College e-mail address. Any incoming e-mail should be considered to be suspicious and attachments not opened unless the author and web origin are known.

Staff should be aware that all e-mails are subject to Freedom of Information requests. Staff should therefore ensure that their College e-mail account is used only for professional work-based communication.

SOCIAL MEDIA/NETWORKING AND PERSONAL PUBLISHING

GENERAL PRACTICE AND ADVICE FOR STAFF AND STUDENTS IN THE USE OF SOCIAL MEDIA

For the purposes of this policy, social media is defined as any interactive online media that allow parties to communicate instantly with one another or to share information in a public forum. Examples include Twitter, Facebook and LinkedIn. Social media may also include blogs and video and image-sharing websites such as WordPress, YouTube and Flickr.

However, there are many more examples of social media and this is a constantly developing area of communication. College staff should adhere to these policy guidelines in relation to any social media that they use in relation to the undertaking of their professional duties and in relation to how the implications of their personal online activity may impact on their professional life.

Whilst social media is a powerful tool for building relationships and contacts, it can also be used for negative purposes such as bullying and grooming. The College is very clear on its approach to the use of social media by staff and students.

- students are not permitted to access social networking sites during school hours. Access for all students is therefore blocked on the College network
- members of staff are not permitted to make or maintain contact with current Salesian College students through any form of social media (in accordance with the College's *Safeguarding Children Policy*)
- it is recommended that all staff and students at the College set the privacy levels on their social media accounts to an appropriately strict level, i.e. you should have total control and knowledge of who views your pictures/private information/friends etc.
- members of staff should be aware that it is relatively easy for pupils to track them down on social media. For instance, it is very possible that a pupil could be a "Friend of a Friend". Staff are therefore

advised to not post anything on social media which could bring their professional standing into disrepute or in any other way compromise them
- staff and students should be fully aware that any picture of them, or comment originating from them, can be copied and reproduced anywhere else on the internet. Others can copy pictures or comments and/or can email these or otherwise broadcast to whomever they wish. In particular, a "profile picture" can be seen by everyone unless access is specifically limited by the account owner
- note that anyone can set up a Social Media account, using any name. It is not unknown for pupils to pose as someone else, in order to befriend staff members on Social Media or to even impersonate a member of staff. In these cases, the motive is nearly always mischievous. If staff or students believe that either they or someone they know is being impersonated on social media, then it is possible to contact the relevant company (e.g. Facebook/Twitter/Instagram) to report the account as an imposter. Staff should inform the Deputy Headteacher that an imposter account exists.
- No individual should use the school email address when setting up personal social media accounts.

USE OF SOCIAL MEDIA IN A PROFESSIONAL CAPACITY

Social media can be a very powerful marketing and communication tool. As such its use in a professional capacity is acceptable, but any member of the College staff who wishes to use social media in this way must obtain permission from the Headmaster. In setting up and using a professional account, staff must:

- clearly define the purpose, type of communication and membership of the site (e.g. for communication during a College trip)
- seek advice and support from the IT Support team as necessary
- be responsible for the monitoring of all content throughout the site
- be responsible for removing any inappropriate content
- be responsible for restricting site membership
- ensure that the site is private and that it cannot be accessed by anyone else, other than the intended members, without invitation
- ensure that the site is removed from the internet when it is no longer needed

Any staff using any Social Media sites made in a professional capacity must not allow any postings to:

- bring the school into disrepute
- breach confidentiality
- breach copyrights of any kind
- bully, harass or be discriminatory in any way
- be defamatory or derogatory

MANAGING VIDEO-CONFERENCING

Video-conferencing technology may be used for the purposes of teaching and learning. Students must not make or answer video-conference calls in school without permission from a member of staff. All video-conferencing involving students must be supervised at all times by a member of staff. Video-conferencing instigated through the College should be via Microsoft *Teams* unless there is a specific reason to use a different platform. Use of a different platform must be approved by the IT Manager.

LIVE REMOTE LEARNING AND MICROSOFT *TEAMS*

Should the need arise, live remote learning activities will take place via Microsoft *Teams.* Use of *Teams* ensures that membership is restricted to members of the College community. Any class teams created for remote learning should be "private" Teams, meaning that only Team Owners (teachers) can add members. Other, non-class Teams, may be "public" Teams, meaning that any member of the College community can join. Use of the term "public" by Microsoft is misleading as membership is still restricted to members of the College community. Staff and students will be issued with 'Remote Teaching and Learning Procedures' which detail protocols for this in the event that these are required.

As per the Internet Acceptable Use Policy, students should not take images or make recordings of any Teams lessons.

The College system allows students to set up Teams to communicate with each other. This functionality has not been disabled as it is the College's view that should we deny students this functionality, students would simply use other, less secure platforms which we could not monitor.

DIGITAL MEDIA AND AGE APPROPRIATENESS

We now have unprecedented access to a wide range of media to use in the classroom, for example:

- Films
- TV programmes
- Radio programmes
- DVDs
- Images, film clips and music/audio clips accessed through the internet

These resources are collectively referred to as media in this section of the policy.

Media content can be shown in every teaching space using either a DVD player, computer or iPad. Staff must ensure that they adhere strictly to the age classification of any media shown and ensure that there is a licence to show such media. If members of staff have any doubt about the suitability of any media, permission must be sought from the Headmaster or Deputy Headteacher before such media is shown. Staff should check details in the *Use of Internet, DVD and Licences* section of the Staff Handbook

MANAGING EMERGING TECHNOLOGIES

The College continually examines emerging technologies with regard to their benefits to teaching and learning and a full analysis will take place before rolling out any new technologies for use in the classroom.

IPADS

Responsible User Policies have been written to govern the use of iPads at the College. Staff and students must sign to indicate that they have read, understood and agree to comply with the appropriate policy before an iPad will be issued.

- *iPad Responsible User Policy (Staff)*
- *iPad Responsible User Policy (Students)*

Use of iPads in the classroom is governed by a set of rules as given in the students' planners and as posted on the walls of every classroom.

- iPad Classroom Rules

Prior to any new applications being added to the student's iPads, the College will undertake a thorough risk assessment process. The use of cameras within the College, such as those in the student's iPads, will be only be permitted in lessons where the teacher has been given explicit permission. Such photographs will be taken for use in the specific lesson and must never be uploaded to the internet or e-mailed to any third party without the explicit permission of the subject of the photograph and the teacher.

MOBILE TELEPHONES

The use of mobile phones by students within the College is governed by the Colleges' *Mobile Phone Policy*.

Staff should not use personal mobile phones to communicate with students, unless it is an emergency. Staff should not store students' mobile phone numbers on their personal phones.

The College possesses a number of mobile phones which can be loaned to staff during trips and visits. Wherever possible, staff should use a College phone if communication with an individual student is necessary.

HANDLING E-SAFETY MISUSE AND COMPLAINTS

Specific complaints should in the first instance be reported to the Deputy Headteacher who will liaise with Heads of Department, Heads of Year, the Senior Deputy Headteacher and the Headmaster as appropriate.

The College will not tolerate the misuse of technology to bully, harass, or belittle another pupil and such behaviour will be sanctioned in accordance with the College's Anti-Bullying Policy.

Illegal activities or activities that are inappropriate in a College context, may be reported to the police and/or the Local Authority Designated Officer. If the College discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Command.

COMMUNICATING THIS POLICY TO STUDENTS

Appropriate elements of the e-Safety Policy are shared with pupils via the *Internet Acceptable Use Policy* and the *iPad Responsible Use Policy (Students)*.

e-Safety rules are posted in all networked rooms whilst iPad usage rules are displayed in all classrooms. Students are routinely informed that network and internet use will be monitored. A range of curricular and extra-curricular opportunities to develop awareness of e-Safety issues and how best to deal with them is provided annually for pupils through the PSHE Programme, Computing lessons and through presentations by external agencies.

COMMUNICATING THIS POLICY TO STAFF

All staff are given access to the College's e-Safety Policy in the Staff Handbook. Staff are asked to read the policy at the beginning of each academic year and are asked to sign to indicate that they have understood and accept its terms and conditions and that they agree to work within the specified guidelines.

COMMUNICATING THIS POLICY TO PARENTS

The e-Safety policy will be made available to parents on the College web-site.