DE LA SALLE COLLEGE

E-SAFETY POLICY

"TURN MY EYES FROM LOOKING AT WORTHLESS THINGS; AND GIVE ME LIFE IN YOUR WAYS."

PSALM 113:97

Compiled by: The Head of College	Last Reviewed: June 2023
Policy Holder: Mr M. Le Moignan	Revision date: June 2024
Oversight Governor: Tracey Townsend	Verification date: Spring 2024

Contents

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our boys with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At De La Salle College we understand the responsibility to educate our pupils on e-safety and data security issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

De La Salle College holds personal data on learners, staff and other people to help us conduct our day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the college. This can make it more difficult for our college to use technology to benefit learners.

Everybody in the college has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the college (such as PCs, laptops, Smart phones, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto college premises (such as laptops, mobile phones, camera phones, smart phones and portable media players, etc.).

E-Safety

E-Safety - Roles and Responsibilities

The E-Safety policy, supported by the college's Acceptable User Policies (AUP's) for staff, governors, visitors and pupils, is to protect the interests and safety of the whole college community.

Outline

Headmaster of College	Mr J Turner	j.turner@dls-jersey.co.uk
Vice Headmaster of College	Mr K McGinty	k.mcginty@dls-jersey.co.uk
Headmaster of Primary School	Mr G Coutanche	g.coutanche@dls-jersey.co.uk
SIRO	Mr S Barrett	s.barrett@dls-jersey.co.uk
DPO	Mr D Washington	d.washington@dls-jersey.co.uk
E-Safety Coordinator	Mr M Le Moignan	m.lemoignan@dls-jersey.co.uk
Network Manager	Mr D Townsend	d.townsend@dls-jersey.co.uk
Child Protection Officer	Mr A Cook	a.cook@dls-jersey.co.uk
Police Liaison Officer	PC J Carter	SAYF@jersey.pnn.police.uk
SENCO	Mrs N Jones	n.jones@dls-jersey.co.uk

Headmaster, SLT and Governors

- The Headmaster is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- They are also responsible for ensuring that pupils and students are taught how to use ICT tools such as the internet, email and social networking sites safely and appropriately.
- The Headmaster will ensure that there is a system in place to allow for monitoring and support of those within the college who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The SIRO, SLT and Governors will receive regular monitoring reports from the E-Safety Co-ordinator.
- The Headmaster and another member of the SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headmaster is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children via the learning platform, have adequate information and guidance relating to the safe and appropriate use of this on-line facility.
- SLT and Governors are updated by the Headmaster/SIRO/E-Safety Coordinator so that they understand the issues and strategies at our college in relation to local and national guidelines and advice.

SIRO

The SIRO is a senior member of staff who is familiar with information risks and the college's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- Oversee and work with the E-safety Coordinator and DPO to ensure a full holistic and cohesive approach to how information risk is managed.
- To understand how the strategic business aims and objectives of the College may be impacted by information risks.
- Ensure that they are kept up to date and briefed on all information risk issues affecting the College and any business partners.
- Meet regularly with E-safety Coordinator, DPO, IT Manger, and other staff members to ensure any risk is managed effectively.
- Oversee and co-ordinate any new e-safety or technical changes to development of the College.
- Review and agree actions in respect of identified information risks.
- Ensure that the College's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
- Provide a focal point for the support, escalation, resolution and/or discussion of information risk issues, policy breaches and data errors.
- To ensure and oversee that all E-safety and GDPR policies and procedures and fully implemented.
- The SIRO in this college is Mr S Barrett (September 2019).

E-Safety Coordinator

The E-Safety Coordinator's roles and responsibilities include:

- Developing an e-safe culture throughout the college as part of safeguarding, which is in line with National/Government of Jersey best practice recommendations.
- Ensure that e-safety is clearly identified and established as part of the roles and responsibility of the SLT and Governing body.
- Act as a named point of contact on all e-safety issues and liaise with other members of staff as appropriate.
- Audit and evaluate current practice to identify strengths and areas for improvement.
- Keep up-to-date with current research, legislation and trends in e-safety and online activities. This may include accessing appropriate training and using a range of approaches to enable them to understand the role of new technology as part of modern British society and the wider safeguarding agenda.
- Lead an e-safety committee and hold termly meetings to discuss internal and external e-safety issues that may have impact on the college.
- Embed e-safety in staff training and CPD by ensuring that all members of staff receive up-to-date and appropriate e-safety training (at least annually and as part of induction) which sets out clear boundaries for safe and professional online conduct.
- Ensure that there is an age and ability appropriate e-safety curriculum that is embedded, progressive, flexible and relevant which engages children's' interest and promotes their ability to use technology responsibly and to keep themselves and others safe online.
- Ensure that the setting participates in local and national events to promote positive online behaviour. E.g. Safer Internet Day, STEM Cyber Security events.
- Ensure that e-safety is promoted to parents, carers and the wider community through a variety of channels and approaches.
- Ensure there are robust reporting channels for the community to access regarding e-safety concerns, including internal, local and national support.

- To ensure that age-appropriate filtering is in place, which is actively monitored. This is also a responsibility of the Network Manager.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- Work with the SIRO and DPO to ensure that practice is in line with legislation.
- Produce appropriate resources that can be used to maintain e-safety integrity throughout the college and ensure that they are widely available to all members of the college. E.g. E-Safety Incident Report Form and AUP's.
- Liaise with the local authority and other local and national bodies as appropriate.
- Review and update E-Safety Policies, Acceptable Use Policies and other procedures on a regular basis (at least annually) with stakeholder input and ensuring that e-safety is integrated with other appropriate college policies and procedures.
- Monitor and report on e-safety issues to the SIRO, SMT and Governing body and other agencies as appropriate.
- Produce, distribute and analyse data from an annual whole college e-safety survey. Two surveys are used; one for primary college and one for secondary college. Information gathered from these survey's is discussed in the e-safety committee meetings and used to further the education of teachers, students, parents and carers.
- Monitor the use of BYOD by students in VI form and those with additional needs.
- Monitor the use of college owned devices in lessons.
- Distribute, collect and securely store AUP's for BYOD or college owned electronic devices.
- Monitor the online reputation of the college on social networking sites.

Network Manager/ICT Support Staff

The roles and responsibilities of the Network Manager and ICT Support Staff include:

- Will ensure that the college's technical infrastructure is secure and is not open to misuse or malicious attack.
- Will ensure that the college meets the required e-safety technical requirements and any local/national e-safety guidance that may apply.
- Will ensure that users may only access the network and devices through properly enforced password protection, ensuring that passwords are regularly changed.
- Will ensure that the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single individual.
- Will ensure that the use of the network, internet, VLE, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headmaster/SIRO/E-Safety Coordinator.
- Will ensure that monitoring software and systems are implemented and updated as agreed in college policies.
- Will respond and act upon 'helpdesk' requests made by students and staff within an appropriate timeframe (as described on the helpdesk page).
- Will attend annual events that advertise and support new technologies to ensure that systems and software within the college are up-to-date. E.g. BETTS Show UK.

Teaching and Support Staff

The e-safety roles and responsibilities for all teaching staff, support staff and supply staff include:

- They have an up-to-date awareness of e-safety matters and of the current college e-safety policy and practices.
- They encourage pupils to develop good habits when using ICT to keep themselves safe.
- They have read, understood and signed the college Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or problems to the SIRO/E-Safety Coordinator/Headmaster for investigation/action/sanction.
- Digital communications with students (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using official college systems.
- E-safety issues are embedded in all aspects of the curriculum and other college activities.
- Pastoral staff will promote the safe use of ICT with their students and will be there to support students who require advice or come forward with an e-safety concern.
- They monitor ICT activity in lessons, extra-curricular and extended college activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current college policies with regard to these devices.
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- All online teaching content must be checked before delivery to ensure that websites, online searches, images and videos are age appropriate and suitable for student viewing.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience or break GDPR policy. Please see the 'Data Protection' policy for further information.
- You must not reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site.
- Online gambling, illegal activities or any activity deemed inappropriate by the college is not allowed within the college or on college devices. It is at the Headmaster's discretion on what internet activities are permissible for staff and how this is disseminated.

Pupils

The following e-safety roles and responsibilities apply to students within the college:

- The college has a framework for teaching internet skills in computing lessons.
- The college provides opportunities within a range of curriculum areas to teach about e-safety.
- Students have access to the college network and technologies that enable them to communicate with others beyond the communicate environment.
- Students are responsible for using the college ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to the college systems.
- Students are taught to critically evaluate materials, learn good researching skills and the need to avoid plagiarism and uphold copyright regulations.

- Students must observe software copyright at all times. It is illegal to copy or distribute college software, illegal software from sources or copyright materials from electronic resources (e.g. Kerboodle).
- Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Students should be aware of reporting issues using the 'Confide' button on their profile.
- Pupils are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying through lessons in both PSHE and ICT. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies. E.g. Parent/Guardian/Teacher/Organisations such as Childline or CEOP.
- Students will be expected to know and understand college policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand college policies on the taking/use of images, use of social networking sites and on cyber-bullying.
- Students should understand the importance of adopting good e-safety practice when using digital technologies outside of the college and realise that the college's e-safety policy covers their actions outside of the college grounds, if related to the use of an externally available web-based system, provided by the college.
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual properties which may limit what they want to do but also serves to protect them.
- Online gambling, illegal activities or any activity deemed inappropriate by the college is not allowed within the college or on college devices. It is at the Headmaster's discretion on what internet activities are permissible for students and how this is disseminated.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The college will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website information, Learning Platform information and sharing local/national notifications.

Parents/Carers are responsible for:

- Accessing the college website, Learning Platform, virtual student homework planner and online parents evening system in accordance with the relevant college Acceptable Use Policies.
- Promoting the safe use of online devices both within and outside of the college.
- Ensure that homes are fitted with adequate online security to maintain the safety of their child. Advice is available from the college SIRO, E-Safety Coordinator and Network Manager.
- It is advised that parents recheck any websites that are recommended by staff for homework activities to check their suitability. Parents are advised to supervise work that is completed online or on an electronic device.

E-Safety in the Curriculum

PSHE and E-Safety Roadmap

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

E-safety will be taught directly within the subjects of 'Computing' and 'PSHE'. The aspects of e-safety taught in Computing can be found within the Computing departmental handbook. The aspects of e-safety taught to students in PSHE are highlighted in the exemplar roadmap that is included within this document. There is no national scheme of work for the teaching of e-safety but aspects of e-safety should be built into the PSHE program of study. The college has independently formed a suitable exemplar roadmap that incorporates the individual topics of e-safety ensuring that they are up-to-date and age appropriate, whilst maintaining the ethos of the college.

- ☐ ***APPENDIX: E-SAFETY IN PSHE ROADMAP***

E-Safety Survey

At least once every three years, a whole college e-safety survey will be completed during the week of Internet Safety Awareness day (February). The e-safety survey will provide insight into the students understanding of e-safety and will allow the college to direct further teaching to students and their parents/guardians.

- ☐ ***APPENDIX: E-SAFETY SURVEY***

E-Safety Skills Development

Inset for NQT/RQT/New, Supply and Support Staff

- Where appropriate, new members of staff including NQT, RQT, Support Staff and Supply Staff will undergo mandatory training with the colleges E-Safety Coordinator, with the support of the Network Manager.
- Where appropriate, staff will read, understand and consent to the colleges Acceptable User Policy (AUP) as a part of their introduction.

- ☐ ***APPENDIX: E-SAFETY WALKTHROUGH FOR NQT/RQT/NEW, SUPPLY AND SUPPORT STAFF***

Training

- Staff receive regular information and training on e-safety issues in the form of child protection courses and e-safety courses. These are carried out by local and national external agencies as well as online interactive training.
- Teaching staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.
- Staff have been made aware of individual responsibilities relating to the safeguarding of children with the context of e-safety and know what to do in the event of misuse of technology by any member of the college community.

- Details of ongoing staff training can be found by speaking with the SIRO or E-Safety Coordinator. A set of online, interactive courses are assigned for this purpose to college staff each academic year.

E-Safety Communication

Letters/Newsletters/Posters/Website

In order for the latest e-safety information to be communicated to members of the college, the following will take place:

- E-safety notice board in the staff room will be updated regularly and urgent announcements will be made in the weekly staff briefing and/or communicated by email. This will be completed by the e-safety coordinator or the SIRO.
- E-safety notices will be placed in the parent briefing occasionally, which is emailed to parents on a weekly basis. This will be completed by the e-safety coordinator of the SIRO.
- E-safety notices will be added to the college's Twitter account via the college website. The SIRO will be in charge of adding these to the Twitter account.
- Urgent e-safety announcements will be made to students via their weekly House assemblies.
- General e-safety announcements, updates and reminders will be shown on the college TV screens as digital posters.

Website Links

In order to learn more about e-safety, staff, parents, guardians and students can refer to the following websites. The links to these websites can be found on the new De La Salle College website.

- www.thinkuknow.co.uk
- www.parentsprotect.co.uk/internet-safety.htm
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/
- www.internetmatters.org
- www.compareitech.com
- www.nationalonlinesafety.com
- www.parentinfo.org
- www.saferinternet.org.uk
- www.childnet.com
- www.kidsmart.org.uk
- www.digzen.org
- www.giftedgeek.co.uk/keep-children-safe-online
- www.kooth.com

Safer Internet Awareness Day

Safer Internet Awareness Day (SID) is an international event taking place in February every year, which promotes a safer and more responsible use of online technology and mobile technology by children and young people across the world.

Safer Internet Day will be included as a part of the colleges Theme of the Week (TOTW) during the month of February as close to the date of this event as possible. The SIRO, E-Safety Coordinator or an appropriate guest speaker will discuss the importance of this day/week. This

information/presentation will be rolled out in the weekly House assemblies and will be organised by the E-Safety Coordinator.

Open Evening, Parents Evening and Welcome Evening's

During the course of these events the E-safety coordinator will be present to meet with parents to discuss the e-safety provisions that we put in place at De La Salle College. The Police Liaison Officer for the college may also be present to speak with parents on an informal basis regarding any e-safety matters both within the college and at home.

E-Safety Committee

The aim of the e-safety committee is to meet on a termly basis to discuss any updates or concerns regarding e-safety both within and outside of the college. It is designed to keep all college members up-to-date with the latest e-safety information and minimise the harm that could occur to college members.

The e-safety committee consists of:

- SIRO – Mr S Barrett
- E-Safety Coordinator – Mr M Le Moignan
- DPO – Mr D Washington
- College Police Liaison Officer – PC A Galvin
- College E-Safety Governor – Mr G Zambon
- Network Manager – Mr D Townsend
- Child Protection Officer for the College – Mr A Cook

All minutes for these meetings are recorded and published for staff members in the staff shared area. They can be found in the 'E-Safety' folder. Important matters that arise from the meeting are passed onto the College Headmaster via the SIRO.

Communication of Policy

- This policy will be available for all staff members to view under the 'College Documents' folder in the staff shared area.
- Where appropriate, new members of staff/NQTs/RQTs/support staff/supply staff will be expected to read this policy on initiating their contract and confirm that they have read and understood its content.
- This policy will be available for all parents/guardians to read via the college website. It can be accessed securely via the parent/guardian login page.

Review of E-Safety Policy

- There will be an on-going opportunity for staff to discuss any concerns/issues of e-safety with the E-Safety Coordinator or SIRO.
- This policy will be reviewed every 12 months and consideration given to the implications for future whole college development planning.
- The policy will be amended if new technologies are adopted or the Government of Jersey change the orders or guidance in any way.

- This policy will be read, amended and approved by the Headmaster and E-Safety Coordinator annually, as guided by the dates on the cover page of this document.

Acceptable User Policies (AUP's)

The acceptable User Policies for the college are checked regularly to ensure that they are up-to-date with the recommendations from local and national agencies.

AUP: Primary College – Student

- The Acceptable User Policy for primary college students is worded in such a way that all students have the ability to comprehend the information that it is stipulated.
- Pupils are expected to read and discuss this agreement with their parent/guardian and follow the terms of agreement. Any concerns or explanation can be discussed with their class teacher or the Headmaster of the Primary College.
- The AUP is attached to the welcome pack that all students receive when entering the primary school of the college.
- Any new students to the primary school of the college will have to sign the AUP before having access to the ICT hardware and online access.
- The AUP must be agreed to upon logging in to the college network. Failing to agree to the AUP will result in the user failing to get access.

- ***APPENDIX: AUP: PRIMARY COLLEGE – STUDENT***
- ***APPENDIX: AUP: PRIMARY COLLEGE – LETTER TO PARENTS***

AUP: Secondary College – Student

- The Acceptable User Policy for primary college students is worded in such a way that all students have the ability to comprehend the information that it is stipulated.
- Pupils are expected to read and discuss this agreement with their parent/guardian and follow the terms of agreement. Any concerns or explanation can be discussed with their House Tutor, the E-Safety Coordinator or the SIRO.
- The AUP is attached to the welcome pack that all students receive when entering the secondary school of the college.
- Any new students to the secondary school of the college will have to sign the AUP before having access to the ICT hardware and online access.
- The AUP must be agreed to upon logging in to the college network. Failing to agree to the AUP will result in the user failing to get access.

- ***APPENDIX: AUP: SECONDARY COLLEGE – STUDENT***
- ***APPENDIX: AUP: SECONDARY COLLEGE – LETTER TO PARENTS***

AUP: Staff, Governors and Visitors

- All staff members, governors and visitors (who have access to ICT) of the college must sign the AUP before having access to the college's ICT equipment and online access.

- Any concerns or clarification should be discussed with the E-Safety Coordinator or the SIRO.
- The AUP must be agreed to upon logging in to the college network. Failing to agree to the AUP will result in the user failing to get access.

- ***APPENDIX: AUP: STAFF, GOVERNORS AND VISITORS***

E-Safety Breaches

A breach or suspected breach of policy by a college employee, contractor or pupil may result in the temporary or permanent withdrawal of college ICT hardware, software or services from the offending individual.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting and Incident Log

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the college's SIRO. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy noncompliance must be reported to the college's SIRO and/or the DPO.

The e-safety incident log book is stored safely and securely by the E-safety Coordinator or SIRO. Serious or reoccurring e-safety incidents and complaints are investigated by the SIRO, and other necessary staff/agencies. These matters are recorded on an e-safety incident report form.

- ☐ ***APPENDIX: E-SAFETY INCIDENT REPORT FORM***

Unsuitable and Inappropriate Activities

The following activities have been categorised based on what is acceptable/not acceptable by Jersey Law as well as the views of De La Salle College Jersey. Any activities that take place, that are not found on this list will be deemed acceptable/not acceptable at the discretion of the Headmaster.

- ☐ ***APPENDIX: E-SAFETY UNSUITABLE AND INAPPROPRIATE ACTIVITIES***
- ☐ ***APPENDIX: FLOWCHART FOR MANAGING AN E-SAFETY INCIDENT***

E-Safety Breach Protocol

Responding to Illegal Incidents

Once an e-safety incident report form has been filed and it is established that the incident is of an illegal nature then the SIRO will follow the steps outlines in the Appendix: Flowchart for Managing an E-safety Incident.

Users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be identified immediately and reported to the E-safety Coordinator or the SIRO.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety Coordinator or SIRO, depending on the seriousness of the offence; investigation

by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see Appendix).

Responding to Non-illegal Incidents

Once an e-safety incident report form has been filed and it is established that the incident involves a non-illegal activity, the individual will be spoken to by either the E-safety Coordinator or the SIRO, depending on the nature of the incident.

All incidents will be logged on the e-safety incident report log by the e-safety coordinator and the parents/guardians of the individual will be contacted.

If the incident is of a repetitive or is a more severe non-illegal incident, it may be that the college's Police Liaison Officer is involved with the incident.

Issues of this nature involving staff will be dealt with similarly and may involve discussions with the Network Manager and/or the Headmaster.

Complaints

Complaints and/or issues relating to e-safety should be made to the SIRO or Headmaster. All incidents should be recorded on an e-safety incident report form.

E-Safety Risk Assessment

- Activities involving online media, images from the internet and internet research should be risk assessed using the college 'E-Safety Risk Assessment' form.
- Staff members are responsible for completing their own 'E-Safety Risk Assessment' or they should ask for assistance from the E-Safety Coordinator in order to complete one.
- Completed risk assessments are stored within the 'E-Safety' situated in the Staff Shared area. Staff members have access to these.

☐ ***APPENDIX: E-SAFETY RISK ASSESSMENT FORM***

Storing/Transferring Personal, Sensitive, Confidential or Classified Information

The storage and transfer of personal, sensitive, confidential or classified information is covered in the Data Protection Policy.

Equal Opportunities

Pupils with Additional Needs

The college endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the college's e-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities must be planned and well managed for these children and young people. If in doubt the College's ENCO.

Infrastructure

College Hardware

Staff Computers/Laptops

Staff computers, staff files and personal devices being used for work purposes have the right to be monitored or checked at the discretion of the Headmaster if there is an issue relating to E-safety. Staff files are checked by the Network Manager annually.

ICT Suites

Students using the ICT suites should be monitored by a staff member at all times depending on their year group. Student workstations should be monitored by the staff member present by visual checks or using Impero station. Students are protected by the college filtering systems (Smoothwall and Impero).

Printing/Scanning/Faxing

Staff have individual codes to access the printing and scanning services within the college. Staff should not share these codes with others and should only use their own codes.

Portable Hardware

Bring Your Own Device (BYOD)

Students in VI Form have the option to bring in their own electronic device that can be used for work purposes and can be connected to the college Wi-Fi network. Students have the option of using a laptop or a tablet, however, mobile phones are not accepted devices.

Students with specific educational needs can also apply to bring in and use their own electronic device with the permission of the SENCO and E-Safety Coordinator.

For further information, including the Acceptable User Policy (AUP) for the use of electronic devices (BYOD), please refer to the college's 'Electronic Devices' policy.

College Laptops/Electronic Devices

In reference to the information found above regarding BYOD, students who cannot provide their own device, but require one for their work, can be loaned a college device for the duration of their time in VI form. Students with specific educational needs who are in the same situation can also be loaned a college electronic device.

For further information, including the Acceptable User Policy (AUP) for the use of electronic devices (BYOD), please refer to the college's 'Electronic Devices' policy.

Removable Storage/USB's

Staff/Support Staff

- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the college's responsibility nor the Network Manager's to install or maintain virus protection on personal systems.
- Teaching staff members are provided with an encrypted removable storage device within their welcome pack to the college. This is the only removable storage device that will function and should be used by staff if required.
- Any material that has been transferred to removable storage must be stored securely.
- Any removable media that may hold personal data (of any sort), should be disposed of securely as stated in the Data Protection policy.
- Encrypt all files containing personal, sensitive, confidential or restricted data.
- Ensure hard drives from devices no longer in service are removed and stored securely or wiped clean.

Supply Staff/Interviewees/Guest Speakers

- Supply staff, interviewees and guest speakers will not be able to use personal removable storage on the college devices.
- Individuals can plug their own electronic devices into the projectors in order to use their own removable storage or deliver material directly from the device. Material must be checked by the individual to see that it is appropriate for college use.
- Individuals can send in the material in which they wish to use/deliver in order for it to be checked and put onto the shared area. Material should be passed on to the Network Manager or ICT Support Staff for this to be done.

Students

- Students must use the college's email or remote access facilities to transfer work. They must not bring in work on removable storage devices. These will not work within the college.

Disposal of Redundant ICT Equipment

All redundant ICT equipment that may have held personal data will have the storage media removed to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.

The college maintains an inventory of all its ICT equipment including a record of disposal. The college's disposal record will include:

- Date item disposed of
- Authorisation for disposal
- How it was disposed of e.g. waste, gift, sale
- Name of person and/or organisation who received the disposed item

Monitoring E-Safety

- Authorised staff may inspect any ICT equipment owned or leased by the college at any time without prior notice.

- Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its students, employees and contractors, without consent, to the extent permitted by law.
- Authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.
- Please note that personal communications using college ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.
- College internet access is controlled though the De La Salle College web filtering service.
- Staff and students are aware that college-based email and internet activity can be monitored and explored further if required.
- The college does not allow students access to internet logs.
- The college uses management control tools for controlling and monitoring workstations (as highlighted below).
- If staff or students discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the E-Safety Coordinator/SIRO or teacher as appropriate.
- It is the responsibility of the Network Manager, to ensure that anti-virus protection, filtering services and monitoring software is installed and kept up-to-date on all college machines.
- If there are any issues related to viruses, anti-virus software, filtering services or monitoring software, the Network Manager should be informed immediately.
- Students using ICT equipment within a classroom should be physically monitored on a regular basis (teaching mobile around the classroom) to ensure that suitable activities are being completed on the device.
- Where necessary, staff members can request that students show the work being completed on their electronic device. They may request that students sit in a position within the classroom that allows for easier monitoring throughout the lesson.

APPENDIX: MONITORING E-SAFETY ROLES AND RESPONSIBILITIES FLOWCHART

Smoothwall

- Smoothwall software specialises in the web content filtering, safeguarding and internet security. Smoothwall will block websites and web searches which are considered to be harmful or potentially harmful to the user.
- Smoothwall software is installed on all fixed computing devices within the college.
- All computing devices (fixed, mobile, teacher and student) which are connected to the college network are protected by Smoothwall.

Impero

- Impero protects students with online safety technology, developed to identify the potential warning signs of at-risk behaviour, in line with Ofsted and ISI.
- All fixed machines are protected with Impero, allowing the real-time monitoring of online searches and keyword detection.
- All ICT suites in the college support Impero classroom management, allowing the teacher to have real-time monitoring and control of each device within the classroom.

- Impero is not supported on mobile devices including those owned by staff or students who are connected to the college network.

Computer Viruses

- Never interfere with any anti-virus software installed on college ICT equipment that you use.
- If your machine is not routinely connected to the college network, you must make provision for regular virus updates through the Network Manager or ICT Support Staff.
- If you suspect there may be a virus on any college ICT equipment, stop using the equipment and contact the Network Manager or ICT Support Staff immediately. They will advise you what actions to take and be responsible for advising others that need to know.

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and agree to an Acceptable Use Policy to demonstrate that they have understood the college's E-Safety Policy.
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. In Year 0 students have a generic class log-in. In Year 1 and 2 a private password (weak) and from Year 3 (strong).
- Pupils are not allowed to deliberately access on-line materials or files on the college network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of college networks, CMIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Passwords will change every term. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic lock time for the college network should be no longer than 5 minutes**.**
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer).
- In our college, all ICT password policies are the responsibility of the SIRO and all staff and students are expected to comply with the policies at all times**.**
- Always use your own personal passwords to access computer based services.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

- Passwords must contain a minimum of eight characters (alpha numeric) and include a capital or special character and be difficult to guess.
- User ID and passwords for staff and pupils who have left the college are disabled immediately and removed from the system by September 15th for year 10, 11, 12 and 13 leavers and within one week for anyone else.
- **If you think your password may have been compromised or someone else has become aware of your password report this to the Network Manager and to the SIRO.**

Servers

- Always keep servers in a locked and secure environment.
- Limit access rights.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine's specification.
- Data must be backed up regularly.
- Back-up tapes/discs must be securely stored in a fireproof container.
- Back-up media stored off-site must be secure.

Remote Access

- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access. Refrain from using public computers to use remote access.
- To prevent unauthorised access to the college systems, keep all access information such as IP addresses, usernames and passwords confidential and do not disclose them to anyone.
- Select passwords to ensure that they are not easily guessed. For example, do not use your house or telephone number or choose consecutive or repeated numbers. Refer the section 'Passwords' in this policy.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect college information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-college environment.
- Individuals using remote access must ensure that their electronic devices are locked when not in use. The screen should not be in view of any other person.
- Remote access has a 'time-out' function so that it logs the member of staff out of remote access if there is inactivity for a period longer than 5 minutes.

Virtual College

At certain times it may be that students are required to complete distance learning and work online when outside of the college. It is therefore the college's responsibility to do what is reasonable in order to keep children safe online.

First and foremost, when asking students to distance learn and work online outside of college, the college and staff must adhere firstly and foremost to this Policy, to the Child Safeguarding Policy and the GDPR policy to maintain good practice.

An essential part of distance learning and the online teaching process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. Information with regards online learning will be emailed out to all parents to advise how online learning will operate, where resources can be found and finally to remind parents of e-safety good practice. The students must be reminded and aware that they are able to contact their House Tutor, Head of House or other members of staff should an issue arise. Further, as well as reporting routes back to the College, students will also be signposted to age appropriate practical support from the likes of:

Childline - for support

UK Safer Internet Centre - to report and remove harmful online content

CEOP - for advice on making a report about online abuse

This information and good practice advice for working online can be incorporated into a pro-forma email when the college is working through the Virtual School in order for each student to be aware of it on a daily basis. It can also be emailed to parents in the Primary school.

When distance learning or asking students to work online outside of the college, it is important that we are in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

Other considerations which the college and staff must consider in relation to distance learning and use of online provision is as follows but not exhaustive:

1. Staff to be aware of the Acceptable User Policy.
2. Staff to make students in their class or House group aware of the Acceptable User policy.
3. The importance to consider the age of student in your class, both in terms of the age requirements of the service/product you are using, together with their ability to participate in it.
4. Not all students will have access to technologies that will enable them to participate in distance learning or use online resources. Staff need to consider what solutions you can provide to enable them to continue learning. E.g. Loan devices from the college or post assignments/work home.
5. Consider activities carefully when planning – online access within the college will have internet content filtering systems in place that are unlikely to be replicated in the home environment. In Virtual School students should not be directed to any forum or website, such as You Tube, which has not been fully researched by the teacher. The teacher must ensure that, to the best of their knowledge, the website page they are sending is age specific and would not allow students to come into contact with third parties or view unsuitable material. The teacher, where possible, should advise students and/or parents not to navigate away from the resource sent.
6. Members of staff may choose to create videos to share information, conduct a virtual assembly, lead a prayer or virtual worship opportunity, or provide tutorials to support

remote teaching and learning. Videos should only be uploaded to the school's official Vimeo account by liaising with the Assistant Headteacher responsible for Client Relations or uploaded onto Tapestry for Early Years, subject to the signed agreement with parents. No other video hosting sites should be used, and all content must comply with college's policies for safeguarding and e-safety. It should be understood that all videos will be accessible in the public domain, and commenting should not be made available on any video posted.

Any queries or concerns should be addressed with the College E-safety Co-ordinator or College SIRO.

Online Homework Diary

The online homework diary (Student Manager) has been operational as of 2022 and is used by secondary school staff and students..

- Staff must ensure that the homework details are input correctly with adequate detail and correct dates.
- Staff should ensure that support sessions and demerits being logged contain the correct student details and are written in a professional manner.

Staff must not reveal details of other students in their sanctions when sending information to parents.E-Mail

The use of e-mail within De La Salle is an essential means of communication for both staff and pupils. In the context of college, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between colleges on different projects, be they staff based or pupil based, within college or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

Managing Email

- The college gives all staff their own e-mail account to use for all college business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all e-mail is filtered and logged and if necessary, all e-mail histories can be traced. The college e-mail account should be the account that is used for all college business.
- Under no circumstances should staff contact pupils, parents or conduct any college business using personal e-mail addresses.
- The college requires a standard disclaimer to be attached to all external e-mail correspondence.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on college headed paper. All emails to parents or guardians should be

formal in nature and avoid the use of first names, even if the parent/guardian is well known to the staff member.

- Staff sending e-mails to external organisations, parents or pupils are advised to cc the Headmaster, Line Manager, Head of Department or Head of House.
- Pupils may only use college approved accounts on the college system.
- E-mails created or received as part of your college job will be subject to disclosure in response to a request for information.
- Secondary College students have their own individual college issued accounts. Primary College students in key stage one do not have a college e-mail.
- The forwarding of chain letters is not permitted in college.
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the SIRO if they receive an offensive e-mail.
- Secondary College students are introduced to e-mail as part of the ICT Scheme of Work.
- However you access your college e-mail (whether directly, through webmail when away from the office or on non-college hardware) all the college e-mail policies apply.

Sending e-Mails

- If sending e-mails containing personal, confidential, restricted or financially sensitive data to external third parties or agencies, refer to the section “Emailing Personal, Sensitive, Confidential or Restricted Information”.
- Use your own college e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- An outgoing e-mail greater than twenty megabytes (including any attachments) is likely to be stopped automatically.
- College e-mail is not to be used for personal advertising.

Receiving e-Mails

- Check your e-mail regularly.
- Never open attachments from an untrusted source. Consult the Network Manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- Regularly clean through your emails and delete emails in the ‘Trash’ folder.

E-mailing Personal, Sensitive, Confidential or Restricted Information

- Assess whether the information can be transmitted by other secure means before using e-mail. E-mailing restricted data is not recommended and should be avoided where possible.
- The use of Hotmail, Gmail or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted.
- Where your conclusion is that e-mail must be used to transmit restricted data:

- Obtain express consent from the Headmaster to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to email requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

- ***Please note that any college related information sent by any email is subject to the provisions of GDPR and maybe subject to Freedom of Information Requests***
- If in doubt about any of these issues, please contact the DPO.

Staff Folders and Shared Area

- Staff personal data should not be stored within the staff folders or shared area.
- Staff folders and the shared area should not be abused by staff or students and uploading of material onto these areas should be carefully thought through.
- Staff folders and the shared area will be monitored regularly by the Network Manager.

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the college and therefore no longer have authorised access to the college's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the college has left.
- Staff members who are responsible for roles involving exam board material (AQA, OCR, Edexcel, Pearson) must regularly ensure that only current members of staff have access and that access levels are appropriate.
- Prompt action on disabling accounts will prevent unauthorised access.
- Regularly change generic passwords to avoid unauthorised access.

Telephones/Mobile Phones

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, tablets, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and then risk assessed before use within the college is

allowed. De La Salle manages the use of these devices in the following ways so that users exploit them appropriately.

Staff/Support Staff – College Devices

- You are responsible for the security of your college mobile phone. Always set the PIN code on your college mobile phone and do not leave it unattended and on display (especially in vehicles).
- Report the loss or theft of any college mobile phone equipment immediately.
- The college remains responsible for all call costs until the phone is reported lost or stolen.
- You must read and understand the user instructions and safety points relating to the use of your college mobile phone prior to using it.
- College SIM cards must only be used in college provided mobile phones.
- All college mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.
- You must not send text messages to premium rate services.
- All outgoing phone calls that are not answered should be reported to the college reception to inform them that a return phone call may take place.
- The sending of inappropriate text messages between any members of the college community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the college community.
- Where the college provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used.

Staff/Support Staff – Personal Devices

- The college allows staff to bring in personal mobile phones and devices for their own use.
- The college is not responsible for the loss, damage or theft of any personal mobile device.
- Personal devices should not be left unattended and should be locked when not in use.
- Staff must not take and/or store photos or videos of student activities or data involving students on their personal devices.
- During class outings/trips staff members will take their mobile phone, which is to be used for emergency purposes only.
- Only designated school devices which include staff school phones or department/Pre-Reception and reception cameras and iPads are to be used to take any photo within school or on outings.
- All photos/videos must be downloaded onto the school shared system and deleted.

Students – Personal Devices

- The context of 'electronic devices' includes mobile phones, laptops, gaming consoles, headphones and smart watches.
- Students are allowed to bring personal devices into the college but must not use them for personal purposes during school hours.
- Student devices should not be visible within the college.
- Students seen using their device should be reminded by staff to put their device away or risk it being confiscated.

- It is down to the discretion of the teacher if they wish to allow students to listen to music on their personal devices during their lesson. In this case, 'aeroplane mode' should be active, music should be on 'shuffle' and devices should not be visible. The teacher must be vigilant and report and relevant e-safety issues with the e-safety coordinator or SIRO.
- This technology may be used, however for educational purposes, as mutually agreed with the Headmaster. The device user, in this instance, must always ask the prior permission of the bill payer.
- The college is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the college community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the college community.
- Users bringing personal devices into the college must ensure there is no inappropriate or illegal content on the device. (However, we are aware that it is difficult to 'police' Smart phones).
- Students who are persistent in using their personal device or misuse their device may have the device confiscated for the remainder of the school day. It will be stored safely at the college reception where it can be collected at 15.30. Other guidelines may apply to repeat offenders (see section on 'E-Safety Breaches').

Video Conferencing and MS Teams

- Video conferencing may be used by staff members for lessons or meeting purposes. Software such as Microsoft Teams are preferred. Staff members should be aware of the potential e-safety issues surrounding these calls and can refer to Appendix: A Guide to the Safe Use of Video Conferencing and Virtual Lessons – Staff.
- Students will be allowed the use of Microsoft Teams which is currently under development within the college. Students and parents will receive updates and tutorials on the use of this software as its use progresses within the college. Students and parents must be aware of the potential e-safety implications and freer to Appendix: A Guide to the Safe Use of Virtual Lessons – Parents & Students.

- ***APPENDIX: A GUIDE TO THE SAFE USE OF VIDEO CONFERENCING AND VIRTUAL LESSONS – STAFF***

- ***APPENDIX: A GUIDE TO THE SAFE USE OF VIRTUAL LESSONS – PARENTS & STAFF***

Copyright and Plagiarism

- All staff and students must abide to the copyright and plagiarism laws and/or regulations stated by the publisher.
- Staff are independently responsible for checking the regulations of each publisher before copying information or resources.

Web 2 and Social Networking

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However

it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The college endeavours to deny access to social networking sites to students within school.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Students are asked to report any incidents of bullying (including cyberbullying) to the college.

Virtual Private Networks (VPN's)

- Students should not bypass the college network by using Virtual Private Network technology on either college or personal devices.
- Students found to be using VPN technology may be reported to the E-Safety Coordinator or SIRO and will be subject to the disciplinary procedure as described in the 'College Actions and Sanctions' section of this policy.
- Students should not set up private hotspots on their mobile devices to allow internet access to other individuals.

Webcams and CCTV

- The college uses CCTV for security and safety.
- The only people who can authorise access to CCTV are the Headmaster, the Primary School Headteacher (GCE), the SIRO (SBT), the Head of Behaviour Management (ACK) and Head of Pastoral (CWN).
- Notification of CCTV use is displayed at the front of the college.
-
- CCTV requests should be made using the correct requisition form that can be found in the staff room. A file of such requests will be kept by the Network Manager.
- We do not use publicly accessible webcams in the college.
- Webcam footage is only used in a reactive manner.

Appendix

E-safety in PSHE Roadmap Exemplar

- See 'Staff Shared Area – College Documents – E-Safety – PSHE.

E-Safety in PSHE
De La Salle College

Road Map 2020-2021

Years 1,2,3	Years 4,5,6	Year 7	Year 8	Year 9	Year 10	Year 11	Year 12	Year 13
Role of ICT	Introduction to Internet and Websites	Acceptable User Policy (AUP) at DLS Secondary School	Online Role Models	Mobile Phone Safety	Sex and Relationships	Fake News	Cyber Crime Copyright, Fraud, Plagarism, Piracy	Extremism and Radicalisation
Introduction to Computers	Safe use of Search Engines		Peer Pressure from Online	Online Relationships	Pornography	Using and Sending Emails	Illegal Downloads	Online Profiles and Self-Image (Work Profiles)
Introduction to Electronic Devices	Online Safety and Filtering Systems (Home, Online, School) / Parent Involvement		Self-esteem Online	Online Gaming and Chatrooms	Abuse		File Sharing Services	CV's and Sharing CV's Online (LinkedIn, Job Agencies)
Acceptable User Policy (AUP) at DLS Primary School		Radicalisation and Extremism Introduction		Introduction to Cybercrime	Sexting		VPN's	GDPR at Home and in the Workplace
		E-Safety Keywords: Phishing, Bombing, Trolling, Sexting, Cyberbullying, Sphoofing, Spamming, Flaming			Safe Online Communication (content to be spread across Y9,Y10 & Y11) Comments, Gaming, Bullying, Harrassment, Photos, Consequences, The Law			Income Tax and Pensions
		Mobile Phone Safety						
KS1 E-Safety Survey	KS2 E-Safety Survey	KS3 and KS4 E-Safety Survey					KS5 E-Safety Survey	

E-Safety Survey

- See 'Staff Shared Area – College Documents – E-Safety – College Survey and Results. A primary and secondary survey document can be found in this area. It is distributed to staff and students anonymously using Survey Monkey.

E-Safety Walkthrough for NQT/RQT/New, Supply and Support Staff

- See 'Staff Shared Area – College Documents – E-Safety – Inset and New Staff.

Open Evening and Welcome Evening Presentation

- See 'Staff Shared Area – College Documents – E-Safety – Welcome Evening and Open Evening.

AUP: Primary College – Student

Primary Student
Acceptable Use Agreement / E-Safety Rules

- I will only use ICT in school for school purposes.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ guardian contacted if a member of school staff is concerned about my E-safety.

Pupils are expected to read and discuss this agreement with their parent or guardian and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Mr Coutanche.

AUP: Primary College – Letter to Parents

DE LA SALLE COLLEGE

Wellington Road · St Saviour

Jersey JE2 7TH · Channel Islands

Dear Parent/ Guardian

Use of the Internet by Pupils

As part of our drive to personalise learning and to support learning opportunities within the school, your child, will at appropriate times, be given access to the Internet as an information source, a communications tool and a publishing medium.

The Internet has become a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to support the classroom teacher and the learner is significant and will continue to grow.

Although there are concerns about children having access to inappropriate material via the Internet, the school takes a range of measures to minimise these risks. A filtering system is in operation, which restricts access to inappropriate materials, and this is supplemented by an Internet safety programme for all pupils which teaches the safe and appropriate behaviours to adopt when using the Internet, email and other technologies

Attached to this letter is a copy of the school's Acceptable Use Policy. All users of school computer equipment are expected to abide by this policy.
Where it is evident that the guidelines of the e-safety policy are not being followed, the child concerned will be spoken to and depending upon the seriousness of the breach, appropriate action taken and parents informed.
In extreme cases, the child's access to the learning platform and use of ICT within the school could be suspended.

The school's policy on the use of computers, including the use of the Internet is available for parents to inspect. Should you wish to discuss any aspect of Internet use, please contact me to arrange an appointment.

Yours sincerely

Headteacher

Secondary Student
Acceptable Use Agreement / E-Safety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/Learning Platform with my own user name and password.
- I will follow the schools data handling policy (available on the College website) and not reveal my passwords to anyone.
- I will only use my school e-mail address in school.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will only access the internet through the School provided connection and not by other mobile technologies.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone I chat with online unless this is part of a school project approved by my teacher.
- Images of pupils and/or staff will only be taken, stored and used for school purposes in line with the school data handling policy and not be distributed outside the school network without the permission of the relevant teacher who will have consulted with the DPO.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring De La Salle into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.

- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other related technologies is monitored and logged and can be made available to my teachers.
- I will, when using the remote access facility, abide by all of the above.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/guardian may be contacted.

Pupils are expected to read and discuss this agreement with their parent or guardian and follow the terms of the agreement. Any concerns or explanation can be discussed with their House Tutor or Mr Barrett, SIRO.

AUP: Secondary College – Letter to Parents

DE LA SALLE COLLEGE

Wellington Road · St Saviour

Jersey JE2 7TH · Channel Islands

Dear Parent/ Guardian

Use of the Internet by Pupils

As part of our drive to personalise learning and to support learning opportunities within the school, your child, will at appropriate times, be given access to the Internet as an information source, a communications tool and a publishing medium.

The Internet has become a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to support the classroom teacher and the learner is significant and will continue to grow.

Although there are concerns about children having access to inappropriate material via the Internet, the school takes a range of measures to minimise these risks. A filtering system is in operation, which restricts access to inappropriate materials, and this is supplemented by an Internet safety programme for all pupils which teaches the safe and appropriate behaviours to adopt when using the Internet, email and other technologies

Attached to this letter is a copy of the school's Acceptable Use Policy. All users of school computer equipment are expected to abide by this policy.
Where it is evident that the guidelines of the e-safety policy are not being followed, the child concerned will be spoken to and depending upon the seriousness of the breach, appropriate action taken and parents informed.
In extreme cases, the child's access to the learning platform and use of ICT within the school could be suspended.

The school's policy on the use of computers, including the use of the Internet is available for parents to inspect. Should you wish to discuss any aspect of Internet use, please contact me to arrange an appointment.

Yours sincerely

Headteacher

AUP: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT within school or in a professional context. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr S Barret, Senior Information Risk Officer.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head.
- I will comply with the data handling policy and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will not use social networking sites to communicate with students.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school, or handed to a 3rd party, when authorised by the DPO. Personal or sensitive data taken off site must be encrypted and comply with the GDPR law (May 2018)
- I will not install any hardware or software without permission of the SIRO.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with the data handling policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the DPO.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and comply with the School's e-Safety and data handling policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I give my consent for the College to use images of myself on the School website and other School publications.

User Signature (Governors)

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name ……(printed)

E-Safety Incident Report Form

De La Salle College Jersey

Any e-safety incidents should be recorded on the form below. It is only the responsibility of the teacher to report the facts of the incident and not to investigate the matter themselves. All e-safety reports should be passed on to the SIRO (SBT) immediately. In the event of the SIRO not being available, the form can be passed on to a member of SMT or the Headmaster (JTR).
Any lost/stolen electronic devices or security breaches (including username/password details, remote access details, PINs and electronic door cards) must be reported to the DPO (DWN) and SIRO immediately.

Name of Teacher Reporting Incident: _____

Date of Incident: _____

Location of Incident: _____

Name of Student(s)/Staff Involved in Incident:

_____

_____

Basic Details of Incident (recorded by Teacher):

_____

_____

Date Incident Logged by Teacher: _____

Date Incident Passed onto SIRO (SBT): _____

Confirmed Signature by SIRO (SBT): _____

This section of the form is to be completed by the SIRO (SBT). The e-safety reports must be filed by the SIRO and stored securely. All e-safety incidents will be monitored by the Headmaster (JTR) and reviewed annually by the e-safety Governor (GZN). Incidents involving cyber-bullying should be passed on to anti-bullying officer (ACK).

Incident Type Number(s): _____

Detailed Description of Incident:

_____

_____

_____

_____

_____

Immediate Corrective Action:

_____

_____

_____

_____

Further Action (if any):

_____

_____

Date Incident Resolved by SIRO (SBT): _____

Signed by SIRO (SBT): _____

Incident Types

1 – Circumventing the network security

2 – Installing unapproved software

3 – Using other people's profile/email/passwords

4 – Breaching copyright

5 – Uploading College material onto social network

6 – Bullying/cyberbullying or harassment

7 – Racist/sexist/homophobic comments

8 – Violence or terror related material

9 – Alcohol/drugs/smoking/vaping material

10 – Online gambling material

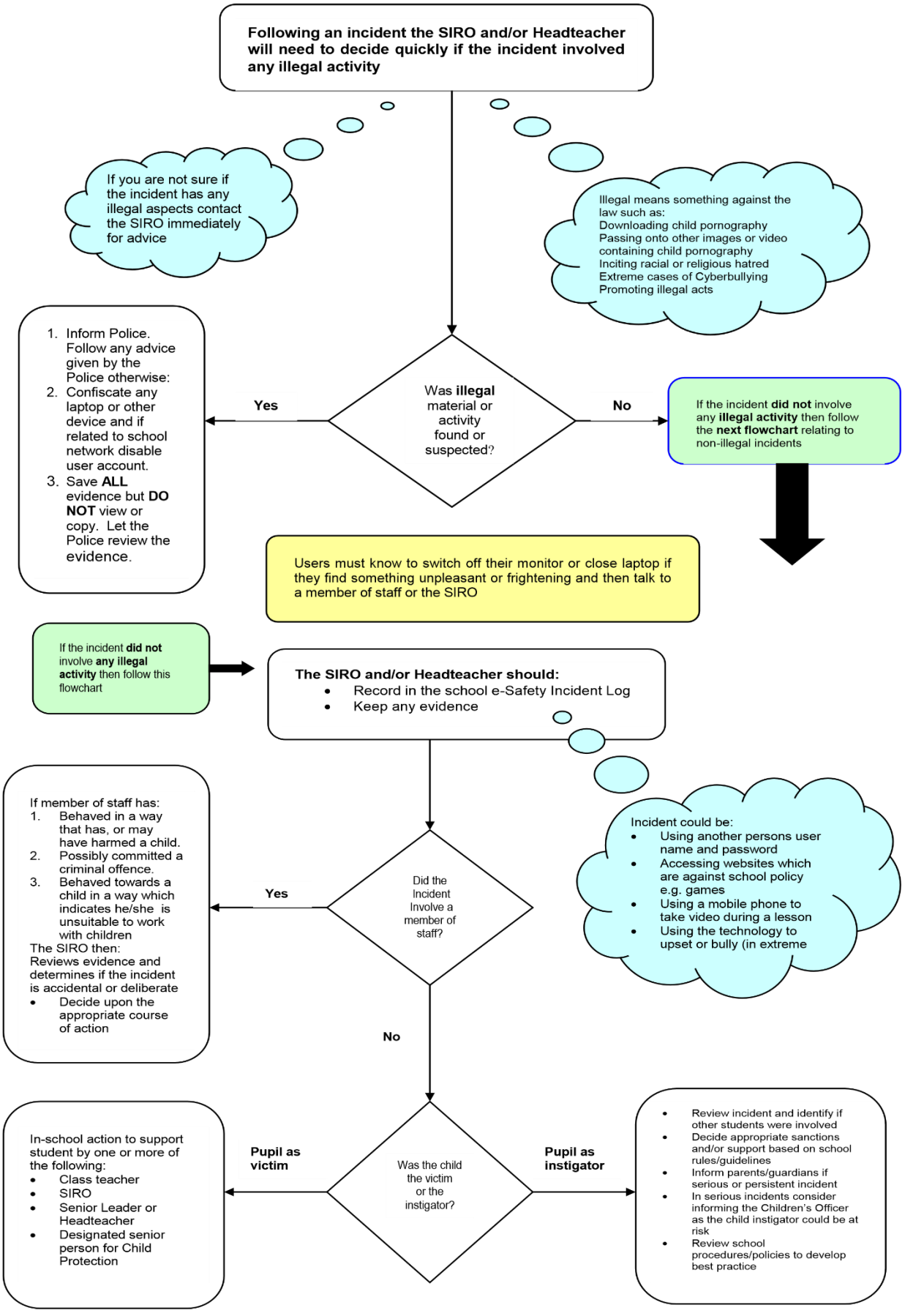
11 – Adult content

12 – Accidental access

13 – Continual noncompliance regarding use of mobile phone on College grounds

14 – Sexting or inappropriate use of mobile phone/electronic devices

15 – Other (please specify)


Following an incident the SIRO and/or Headteacher will need to decide quickly if the incident involved any illegal activity
If you are not sure if the incident has any illegal aspects contact the SIRO immediately for advice
Illegal means something against the law such as:
Downloading child pornography
Passing onto other images or video containing child pornography
Inciting racial or religious hatred
Extreme cases of Cyberbullying
Promoting illegal acts
Was illegal material or activity found or suspected?
Yes
No
1. Inform Police. Follow any advice given by the Police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account.
3. Save ALL evidence but DO NOT view or copy. Let the Police review the evidence.
If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents
Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the SIRO
If the incident did not involve any illegal activity then follow this flowchart
The SIRO and/or Headteacher should:
Record in the school e-Safety Incident Log
Keep any evidence
Incident could be:
Using another persons user name and password
Accessing websites which are against school policy e.g. games
Using a mobile phone to take video during a lesson
Using the technology to upset or bully (in extreme
Did the Incident Involve a member of staff?
Yes
If member of staff has:
1. Behaved in a way that has, or may have harmed a child.
2. Possibly committed a criminal offence.
3. Behaved towards a child in a way which indicates he/she is unsuitable to work with children
The SIRO then:
Reviews evidence and determines if the incident is accidental or deliberate
Decide upon the appropriate course of action
No
Was the child the victim or the instigator?
Pupil as victim
Pupil as instigator
In-school action to support student by one or more of the following:
Class teacher
SIRO
Senior Leader or Headteacher
Designated senior person for Child Protection
Review incident and identify if other students were involved
Decide appropriate sanctions and/or support based on school rules/guidelines
Inform parents/guardians if serious or persistent incident
In serious incidents consider informing the Children's Officer as the child instigator could be at risk
Review school procedures/policies to develop best practice
Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and talk to a member of staff or the SIRO

E-Safety Risk Assessment Template

- See 'Staff Shared Area – College Documents – E-Safety – Risk Assessment.

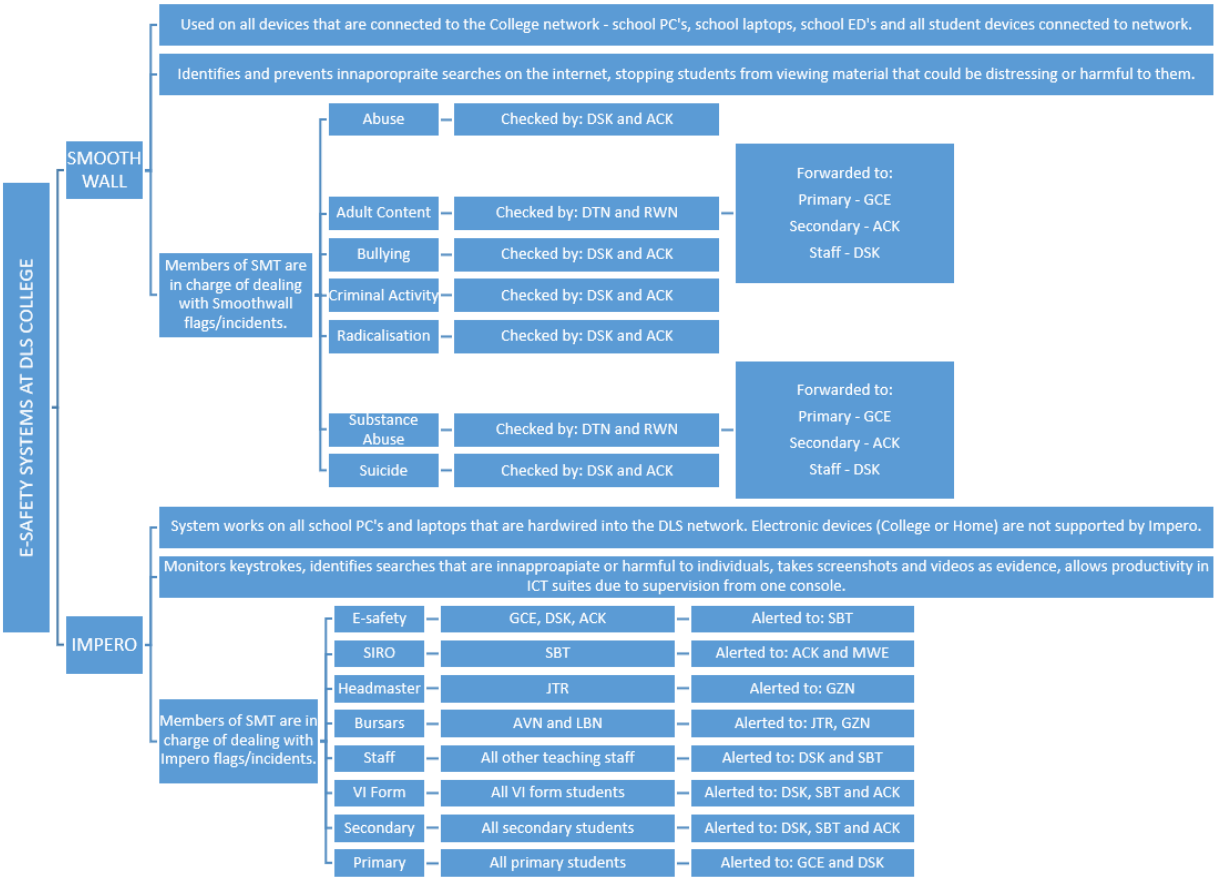
E-Safety Unsuitable and Inappropriate Activities

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:	**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable and illegal**
Child sexual abuse images – the making, production or distribution of indecent images of children Contrary to the Protection of Children's Act 1978					**X**
Grooming, incitement, arrangement of facilitations of sexual acts against children Contrary to the Sexual Offences Act 2003					**X**
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					**X**
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) Contrary to the Public Order Act 1986					**X**
Pornography				**X**	
Promotion of any kind of discrimination				**X**	
Threatening behaviour, including promotion of physical violence or mental harm				**X**	
Any other information which may offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute				**X**	
Using college systems to run a private business				**X**	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college				**X**	
Infringing copyright				**X**	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				**X**	
Creating or propagating computer viruses or other harmful files				**X**	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				**X**	
Online gaming (educational)		**X**			
Online gaming (non-educational)		**X**			

Online gambling				X	
Online shopping/commerce			X		
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting (e.g. YouTube, Vimeo, TES)			X		

E-Safety Monitoring Roles and Responsibilities Flowchart

- See 'Staff Shared Area – College Documents – E-Safety – Roles and Responsibilities.



A Guide to the Safe Use of Video Conferencing and Virtual Lessons – Staff

- See 'Staff Shared Area – College Documents – E-Safety – Microsoft Teams.

A Guide to the Safe Use of Virtual Lessons – Parents and Students

- See 'Staff Shared Area – College Documents – E-Safety – Microsoft Teams