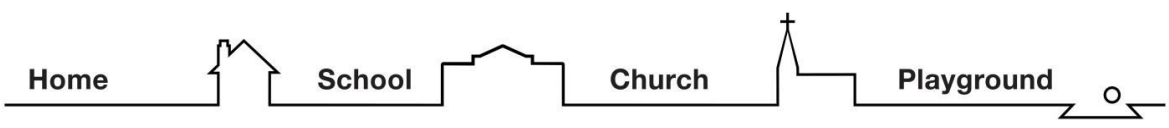
Thornleigh Salesian College

Student Remote Learning Policy

Person responsible	Andrea O'Callaghan
Date of Last Review	October 2020
Ratified by Full Governing Body	October 2020
Date of Next Review	May 2021

Please note: From 22 October 2020 until the end of the 2020/2021 academic year, schools have a legal duty to provide remote education to all students who require it. More details can be found in Appendix A.



Contents:

Statement of intent

At Thornleigh Salesian College, we understand the need to continually deliver high quality education, including during periods of remote learning – whether for an individual student or many. We recognise the importance of maintaining high expectations in all areas of school life and ensuring that all students have access to the learning resources and support they need to succeed.

Through the implementation of this policy, we aim to address the key concerns associated with remote learning, such as online safety, access to educational resources, data protection, and safeguarding.

This policy aims to:

- Minimise the disruption to students' education and the delivery of the curriculum.
- Ensure provision is in place so that all students have access to high quality learning resources.
- Protect students from the risks associated with using devices connected to the internet.
- Ensure staff, parent, and student data remains secure and is not lost or misused.
- Ensure robust safeguarding measures continue to be in effect during the period of remote learning.
- Ensure all students have the provision they need to complete their work to the best of their ability, and to remain happy, healthy, and supported during periods of remote learning.

Signed by:

_____ Headteacher Date: _____

_____ Chair of Governors Date: _____

1. Legal framework

1.1 This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Equality Act 2010
- Education Act 2004
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018

1.2 This policy has due regard to national guidance including, but not limited to, the following:

- DfE (2020) 'Keeping children safe in education'
- DfE (2019) 'School attendance'
- DfE (2018) 'Health and safety: responsibilities and duties for schools'
- DfE (2018) 'Health and safety for school children'
- DfE (2017) 'Special educational needs and disability code of practice: 0 to 25 years'
- DfE (2016) 'Children missing education'

1.3 This policy operates in conjunction with the following school policies:

- Child Protection and Safeguarding Policy
- GDPR Policy
- Special Educational Needs and Disabilities (SEND) Policy
- Behavioural Policy
- Curriculum Policy
- Assessment Policy
- Online Safety Guidance (appended)
- Health and Safety Policy
- Attendance and Absence Policy
- ICT Acceptable Use Policy (appended)
- Staff Code of Conduct

2. Roles and responsibilities

2.1 The Governing Body is responsible for:

- Ensuring that the school has robust risk management procedures in place.
- Ensuring that the school has a business continuity plan in place, where required.
- Evaluating the effectiveness of the school's remote learning arrangements.

2.2 The Headteacher is responsible for:

- Ensuring that staff, parents and students adhere to the relevant policies at all times.
- Ensuring that there are arrangements in place for identifying, evaluating, and managing the risks associated with remote learning.
- Ensuring that there are arrangements in place for monitoring incidents associated with remote learning.
- Overseeing that the school has the resources necessary to action the procedures in this policy.
- Reviewing the effectiveness of this policy on an annual basis and communicating any changes to staff, parents, and students.
- Arranging any additional training staff may require to support students during the period of remote learning.
- Conducting regular reviews of the remote learning arrangements to ensure students' education does not suffer.

2.3 The Director of School Services (DSS) is responsible for:

- Ensuring that the relevant health and safety risk assessments are carried out within the agreed timeframes, in collaboration with the Headteacher.
- Putting procedures and safe systems of learning into practice, which are designed to eliminate or reduce the risks associated with remote learning.
- Ensuring that students identified as being at risk are provided with necessary information and instruction, as required.
- Managing the effectiveness of health and safety measures through a robust system of reporting, investigating, and recording incidents.

2.4 The DSS & Network Manager are responsible for:

- Overseeing that all school-owned electronic devices used for remote learning have adequate anti-virus software and malware protection.
- Ensuring all staff, parents, and students are aware of the data protection principles outlined in the GDPR.
- Ensuring that all computer programs used for remote learning are compliant with the GDPR and the Data Protection Act 2018.

2.5 The Designated Safeguarding Lead (DSL) is responsible for:

- Attending and arranging, where necessary, any safeguarding meetings that occur during the remote learning period.
- Liaising with the Network Manager to ensure that all technology used for remote learning is suitable for its purpose and will protect students online.
- Identifying vulnerable students who may be at risk if they are learning remotely.

- Ensuring that child protection plans are enforced while the student is learning remotely, and liaising with the Headteacher and other organisations to make alternate arrangements for students who are at a high risk, where required.
- Identifying the level of support or intervention required while students learn remotely and ensuring appropriate measures are in place.
- Liaising with relevant individuals to ensure vulnerable students receive the support required during the period of remote working. Ensuring all safeguarding incidents are adequately recorded and reported.

2.6 The Associate Assistant Headteacher (Director of Inclusion) is responsible for:

- Liaising with the Network Manager to ensure that the technology used for remote learning is accessible to all students and that reasonable adjustments are made where required.
- Ensuring that students with EHC plans continue to have their needs met while learning remotely, and liaising with the Headteacher and other organisations to make any alternate arrangements for students with EHC plans and IHPs.
- Identifying the level of support or intervention that is required while students with SEND learn remotely.
- Ensuring that the provision put in place for students with SEND is monitored for effectiveness throughout the duration of the remote learning period.
- Ensuring that the school has adequate insurance to cover all remote working arrangements.

2.7 The Network Manager is responsible for:

- Arranging the procurement of any equipment or technology required for staff to teach remotely and for students to learn from home.
  Ensuring value for money when arranging the procurement of equipment or technology.
- Ensuring that all school-owned devices used for remote learning have suitable anti-virus software installed, have a secure connection, can recover lost work, and allow for audio and visual material to be recorded, where required.
- Ensuring that any programs or networks used for remote learning can effectively support a large number of users at one time, where required, e.g. undertaking ‘stress’ testing.
- Working with the SENCO to ensure that the equipment and technology used for learning remotely is accessible to all students and staff.

2.8 Staff members are responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Reporting any health and safety incidents to the DSS and asking for guidance as appropriate.

- Reporting any safeguarding incidents to the DSL and asking for guidance as appropriate.
- Taking part in any training conducted to meet the requirements of this policy, including training on how to use the necessary electronic equipment and software.
- Reporting any dangers or potential dangers they identify, as well as any concerns they may have about remote learning, to the Headteacher.
- Reporting any defects on school-owned equipment used for remote learning to an ICT technician.
- Adhering to the Staff Code of Conduct at all times.

2.9 Parents are responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Ensuring their child is available to learn remotely at the times set out in paragraphs 9.1 and 9.2 of this policy, and that the schoolwork set is completed on time and to the best of their child's ability.
- Reporting any technical issues to the school as soon as possible.
- Ensuring that their child always has access to remote learning material during the times set out in paragraphs 9.1 and 9.2.
- Reporting any absence in line with the terms set out in paragraph 9.6.
- Ensuring their child uses the equipment and technology used for remote learning as intended.

2.10 Students are responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Ensuring they are available to learn remotely at the times set out in paragraphs 9.1 and 9.2 of this policy, and that their schoolwork is completed on time and to the best of their ability.
- Reporting any technical issues to their teacher as soon as possible.
- Ensuring they have access to remote learning material and notifying a responsible adult if they do not have access.
- Notifying a responsible adult if they are feeling unwell or are unable to complete the schoolwork they have been set.
- Ensuring they use any equipment and technology for remote learning as intended.
- Adhering to the Behavioural Policy at all times.

3. Learning materials

3.1 The school will adopt a range of different teaching methods during remote learning to help explain concepts and address misconceptions easily. For the purpose of providing remote learning, the school may make use of:

- Work set on Google classroom
- Zoom lessons where appropriate

- Email
- Past and mock exam papers
- Current online learning portals such as Oak Academy, BBC portal, GCSE Pod & Seneca Learning
- Educational websites
- Reading tasks
- Live webinars
- Pre-recorded video or audio lessons
- Vulnerable and students with significant SEND, receive a daily contact. To support students with low levels of independence, face to face Zoom sessions are arranged.
- Interventions are delivered online
- HLTAs support staff differentiation of work
- HLTAs create bespoke work packs for students that do not have access to a computer

Full class or bubble provision

Where a teacher's full class is self-isolating, that class teacher will provide online lessons via Zoom for 35 minutes following the student's in school timetable. The link for all such lessons will be placed on Google Classroom. Additional resources such as class PowerPoints will be shared on Google Classroom. In some instances, it is more appropriate for work to be done only on Google Classroom, this will also be the case if the class teacher is absent from school. Students will complete work in exercise books and return these to school for marking on their return. Class teachers may also provide additional feedback live in the lesson, on Google Classroom or via submitted tasks such as quizzes.

Individual student provision

The provision for students self-isolating individually or as a small cohort is to provide a link to all of their lessons as a 'screen share' only. Students will have the opportunity to have some interaction with their teacher at key points in the lesson but the classroom microphone will mainly be on mute. Additional resources will be shared on Google Classroom. Students will complete work in exercise books and return these to school for marking on their return. Class teachers may also provide additional feedback live in the lesson, on Google Classroom or via submitted tasks such as quizzes.

In the situation where a staff member is absent from school because they are self-isolating Zoom lessons may continue.

In the situation where a staff member is absent from school because they are sick then all work will be based on Google Classroom only.

3.2 Teachers will review the DfE's list of online education resources and utilise these tools as necessary, in addition to existing resources.

3.3 Reasonable adjustments will be made to ensure that all students have access to the resources needed for effective remote learning.

3.4 Teachers will ensure the programmes chosen for online learning have a range of accessibility features, e.g. voice-to-text conversion, to support students with SEND.

3.5 The school recognises that interactive lessons are most effective in aiding students' motivation and academic progression and, to this effect, teachers will ensure they regularly recreate aspects of in-person interactivity, e.g. live classes with questioning, eliciting and reflective discussion, to the best of their ability.

3.6 Lesson plans will be adapted to ensure that the curriculum remains fully accessible and inclusive via remote learning.

3.7 The school will review the resources students have access to and adapt learning to account for all students needs by using a range of different formats, e.g. providing work on PDFs which can easily be printed from a mobile device.

3.8 Work packs will be made available for students who do not have access to a printer – these packs will be delivered to families who request them.

3.9 Teaching staff will liaise with the SENCO and other relevant members of staff to ensure all students remain fully supported for the duration of the remote learning period.

3.10 The SENCO will arrange additional support for students with SEND that have significant barriers to learning which will be unique to the individual's needs. This will be primarily done through their assigned member of staff.

3.11 Any issues with remote learning resources will be reported as soon as possible to the relevant member of staff.

3.12 Students will be required to use their own or family-owned equipment to access remote learning resources, unless the school agrees to provide or loan equipment, e.g. laptops.

3.13 For students who cannot access digital devices at home, the school will, where possible, apply for technology support through the DfE.

3.14 Students and parents will be required to maintain the upkeep of any equipment they use to access remote learning resources and the school reserves the right to make a charge for any intentional damage or loss of the device.

3.15 Teaching staff will oversee academic progression for the duration of the remote learning period and will mark and provide feedback on work in line with section 7 of this policy.

3.16 The arrangements for any 'live' classes, e.g. Zoom lessons, will be communicated via Google Classroom no later than 8pm the evening before the allotted time (where this is not possible because of technical or logistical issues the link will be placed as soon as practically possible)

3.17 ICT Support are not responsible for providing technical support for equipment that is not owned by the school.

Food provision

3.18 The school will signpost parents towards additional support for ensuring their children continue to receive the food they need, e.g. food banks.

3.19 Where applicable, the school will continue to provide FSM vouchers for students who are eligible.

Costs and expenses

3.20 The school will not contribute to any household expenses incurred while students learn remotely, e.g. heating, lighting, or council tax.

3.21 The school will not reimburse any costs for travel between students' homes and the school premises.

3.22 The school will not reimburse any costs for childcare.

3.23 If a student is provided with school-owned equipment, the student and their parent will sign and adhere to the ICT Equipment Loan Form prior to commencing remote learning.

4. Online safety

4.1 This section of the policy will be enacted in conjunction with the school's Online Safety Guidance – see attached.

4.2 Where possible, all interactions will be textual and public.

4.3 All students using video communication must:

- Attend every lesson on time.
- Be prepared with pens, paper and calculator.
- Be muted unless invited to turn this off.
- Have the camera turned on.
- Ensure you use your correct name.
- Use a room that has a plain and appropriate background where possible.
- Respect all participants.
- Speak politely to all participants.
- Have their exercise book or paper to write on.
- Not eat or drink during the lesson.

- Only use the ‘chat’ feature with the teacher to ask or answer questions.
- Dress appropriately.
- Join the lesson using the hyperlink provided.
- Must not share the Zoom lesson link with anybody outside of their class.

All staff using video communication must:

- Ensure call security settings are appropriate, eg utilise the waiting room feature, ensure appropriate participant restrictions including in-meeting chat.
- Record and save all lessons as per the school protocol.
- Communicate in groups – one-to-one sessions are not permitted.
- Maintain the standard of behaviour expected in school.
- Not distribute video material without permission.
- Always remain aware that they are visible.
- Ensure the location using to host the zoom call is appropriate, eg ulitise appropriate backgrounds or use a plain background.
- Be aware that student engagement can be harder to judge using webcam feeds.
- Make use of zoom tutorials and guides made available by the ICT & Computer Science Head of Department.

4.4 All staff and students using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programmes as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

4.5 The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for students with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO and the parent.

4.6 Students not using devices or software as intended will be disciplined in line with the Behaviour Policy.

4.7 The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

4.8 The school will inform parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

4.9 The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, and allows for audio and visual material to be recorded or downloaded, where required.

4.10 During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

4.11 The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

5. Safeguarding

5.1 All video interactions with students where there is one member of staff and one student present only will be recorded.

This section of the policy will be enacted in conjunction with the school's Child Protection and Safeguarding Policy, which has been updated to include safeguarding procedures in relation to remote working.

5.2 The DSL and Headteacher will identify 'vulnerable' students (students who are deemed to be vulnerable or are at risk of harm) via risk assessment prior to the period of remote learning.

5.3 The DSL will arrange for regular contact to be made with vulnerable students, prior to the period of remote learning.

5.4 Phone calls made to vulnerable students will be made using school phones or school mobile phone where possible.

5.5 The DSL will arrange for regular contact with vulnerable students once per week at minimum, with additional contact, including home visits, arranged where required.

5.6 All contact with vulnerable students will be recorded on CPOMS.

5.7 The DSL will keep in contact with vulnerable students' social workers or other care professionals during the period of remote working, as required.

5.8 All home visits will:

- Have at least one suitably trained individual present.
- Be undertaken by no fewer than two members of staff.

- Be suitably recorded on CPOMS and the records stored so that the DSL has access to them.
- Actively involve the student

5.9 Vulnerable students will be provided with a means of contacting the DSL, their deputy, or any other relevant member of staff – this arrangement will be set up by the DSL prior to the period of remote learning.

5.10 The DSL will meet (in person or remotely) with the relevant members of staff once per week to discuss new and current safeguarding arrangements for vulnerable students learning remotely in the case of a full school closure.

5.11 All members of staff will report any safeguarding concerns to the DSL immediately.

5.12 Students and their parents will be encouraged to contact the DSL if they wish to report safeguarding concerns, e.g. regarding harmful or upsetting content or incidents of online bullying. The school will also signpost families to the practical support that is available for reporting these concerns.

6. Data protection

6.1 This section of the policy will be enacted in conjunction with the school's Data Protection Policy.

6.2 Staff members will be responsible for adhering to the GDPR when teaching remotely and will ensure the confidentiality and integrity of their devices at all times.

6.3 Sensitive data will only be transferred between devices if it is necessary to do so for the purpose of remote learning and teaching.

6.4 Any data that is transferred between devices will be suitably encrypted or have other data protection measures in place so that if the data is lost, stolen, or subject to unauthorised access, it remains safe until recovered.

6.5 Parents' and students' up-to-date contact details will be collected prior to the period of remote learning.

6.6 All contact details will be stored in line with the GDPR Policy.

6.7 The school will not permit paper copies of contact details to be taken off the school premises.

6.8 Students are not permitted to let their family members or friends use any school-owned equipment which contains personal data.

6.9 Any breach of confidentiality will be dealt with in accordance with the school's GDPR Policy.

6.10 Any intentional breach of confidentiality will be dealt with in accordance with the school's Behavioural Policy or the Disciplinary Policy and Procedure.

6.11 All recorded lessons will be deleted after one full week.

7. Marking and feedback

7.1 All schoolwork completed through remote learning must be:

- Completed in school exercise books where possible and appropriate.
- Returned to school when the child returns.
- Finished when returned to the relevant member of teaching staff.
- Returned on or before the deadline set by the relevant member of teaching staff.
- Completed to the best of the student's ability.
- The student's own work.

7.2 The school expects students and staff to maintain a good work ethic during the period of remote learning.

7.3 Students are accountable for the completion of their own schoolwork – teaching staff will contact parents via email if their child is not completing their schoolwork or their standard of work has noticeably decreased. However parents are responsible for ensuring that students are following their timetable during the day when they are working at home.

7.4 Teaching staff and pastoral teams will monitor the academic progress of students with and without access to the online learning resources and discuss additional support or provision with the Deputy Headteacher as soon as possible.

7.5 Teaching staff will monitor the academic progress of students with SEND and discuss additional support or provision with the SENCO as soon as possible.

7.6 The school accepts a variety of formative assessment and feedback methods, e.g. through quizzes and other digital tools from teachers, and will support them with implementing these measures for remote learning where possible. This variety of assessment methods means that there may be less evident 'ticking' in student books; this does not mean progress is not being monitored.

7.7 The school will log participation and student engagement with remote education, as well as motivation levels and progress, and this will be reported to parents via formal regular reports or, if there is a concern, individually via telephone.

8. Health and safety

8.1 This section of the policy will be enacted in conjunction with the school's Health and Safety Policy.

8.2 Teaching staff will ensure students are shown how to use the necessary equipment and technology safely and correctly prior to the period of remote learning.

8.3 If using electronic devices during remote learning, students will be encouraged to take a screen break between all lessons and spend lunchtime and break time away from screens. If completing a full Zoom timetable students will have a screen break of at least 10 minutes in between lessons.

8.4 If any incidents or near-misses occur in a student's home, they or their parents are required to report these to the Director of School Services or other relevant member of staff immediately via contact@thornleigh.bolton.sch.uk so that appropriate action can be taken.

9. School day and absence

9.1 Students will be present for remote learning by 08:45am and cease their remote learning at 3:10pm from Monday to Friday, with the exception of breaks and lunchtimes, as outlined below

9.2 Breaks and lunchtimes will take place at the following times each day:

- Morning break will take place at 10:30am until 10:50am.
- Lunchtime will take place between either 12.30-13:00pm or 13:00-13.30pm dependent on year group.

9.3 Students are not expected to do schoolwork during the times outlined above.

9.4 Students with SEND or additional medical conditions who require more regular breaks, e.g. sensory breaks, are not expected to do schoolwork during their breaks.

9.5 Students who are unwell are not expected to be present for remote working until they are well enough to do so.

9.6 Parents will inform the attendance line no later than 8:30am if their child is unwell.

9.7 The school will monitor absence and lateness in line with the Attendance and Absence Policy.

10. Communication

10.1 The school will ensure adequate channels of communication are arranged in the event of an emergency.

10.2 The school will communicate with parents via text and email as soon as possible in the first instance to inform them of remote learning. Information will then follow on the school website.

10.3 The Headteacher or Deputy Headteacher will communicate with staff as soon as possible via email about any remote learning arrangements.

10.4 Members of staff involved in remote teaching will ensure they have a working mobile device that is available to take emails or phone calls during their agreed working hours.

10.5 The school understands that students learning remotely have the right to privacy out-of-hours and should be able to separate their school and home lives – communication should only take place during school hours.

10.6 Members of staff will have contact with their Subject Leader once per week if they are working remotely

10.7 As much as possible, all communication with students and their parents will take place within the school hours outlined in section 9.

10.8 Students will have verbal contact with a member of teaching staff at least once per week via group phone call or form Zoom call.

10.9 Parents and student will inform the relevant member of staff as soon as possible if schoolwork cannot be completed.

10.10 Issues with remote learning or data protection will be communicated to the student's form teacher as soon as possible so they can investigate and resolve the issue.

10.11 The students' form teachers will keep parents and students informed of any changes to the remote learning arrangements or the schoolwork set.

10.12 The Headteacher will review the effectiveness of communication on a weekly basis and ensure measures are put in place to address gaps or weaknesses in communication.

11. Monitoring and review

11.1 This policy will be reviewed on an annual basis by the Headteacher.

11.2 Any changes to this policy will be communicated to all members of staff and other stakeholders.

11.3 The next scheduled review date for this policy is May 2021

APPENDIX A

Remote Learning During the Coronavirus (COVID-19) Pandemic

Within the ever-changing circumstances we are currently living through, we must be prepared for local restrictions. If local restrictions apply, the school will implement provision for remote learning to ensure students never miss out on education. We will ensure that our curriculum is inclusive and accessible to all. This policy annex outlines additional measures that will be implemented for delivering remote learning during the pandemic.

1. Legal framework

1.1 This policy has due regard to all relevant legislation, statutory and good practice guidance including, but not limited to, the following:

- DfE (2020) 'Safeguarding and remote education during coronavirus (COVID-19)'
- DfE (2020) 'Adapting teaching practice for remote education'
- DfE (2020) 'Guidance for full opening: schools'
- DfE (2020) 'Get help with technology during coronavirus (COVID-19)'
- DfE (2020) 'Get laptops and tablets for children who cannot attend school due to coronavirus (COVID-19)'
- DfE (2020) 'How schools can plan for tier 2 local restrictions'
- DfE (2020) 'Laptops, tablets and 4G wireless routers provided during coronavirus (COVID-19)'
- Department of Health & Social Care (2020) 'COVID-19 contain framework: a guide for local decision makers'
- DfE (2020) 'Remote education good practice'
- DfE (2020) The Coronavirus Act 2020 Provision of Remote Education (England) Temporary Continuity Direction

1.2 The Headteacher, in collaboration with the governing body, will ensure the school follows the legal obligations regarding remote education, as outlined in The Coronavirus Act 2020 Provision of Remote Education (England) Temporary Continuity Direction. This includes:

- Providing remote education to all students of compulsory school age.
- Providing remote education where it would be unlawful, or contrary to guidance issued from public authorities, for a student to travel to or attend the school.
- Having regard to government guidance issued regarding the delivery of remote education, e.g. the DfE's 'Guidance for full opening: schools'.

2. Contingency planning

2.1 The school will work closely with the LA to ensure the premises is COVID-secure, and will complete all necessary risk assessments – results of the opening risk assessment will be published on the school's website.

2.2 The school will work closely with the local health protection team when local restrictions apply and implement the provisions set within the contingency plan.

2.3 The school will communicate its contingency plans for local restrictions with parents, including which students it will remain open to and which students will receive remote education.

2.4 The school will ensure that remote learning training is regularly refreshed for teachers, and that appropriate trouble-shooting support is available when needed, so the transition from in-person to remote teaching can be as seamless as possible if required.

2.5 If local restrictions are not applied, but a single class or 'bubble' needs to self-isolate, the school will immediately implement remote learning for that group as required.

2.6 The level of remote learning provision required will be based on the government's education four tiers of local restrictions.

These tiers should not be confused with the government's national tiering system for hospitality and household mixing

Where there are no local restrictions in place, these tiers will not apply. The school will remain fully open to all those not required to self-isolate.

Tier 1 local restrictions

2.7 The school will remain open if tier 1 restrictions are in place, and remote learning will not be provided at this time.

Tier 2 local restrictions

2.8 The school will adopt a rota system which will require a combination of remote learning and classroom-based learning to be provided. The rota will allow for two weeks at home and two weeks in school.

2.9 Children of critical workers and vulnerable students will be able to access full-time on-site provision. Attendance for these students will be prioritised and strongly encouraged.

2.10 When considering remote learning in a rota system, teachers will:

- Set assignments so that students have meaningful and ambitious work each day.
- Deliver a planned, coherent and well-sequenced curriculum which allows skills to be built incrementally.
- Assess progress by using questions and other suitable tasks.
- Be clear on how regularly work will be checked.

- Adjust the pace or difficulty of what is being taught in response to questions or assessments, including, where necessary, revising material or simplifying explanations to ensure students' understanding.

2.11 Students who will be unable to engage effectively in remote education at home due, e.g. to a lack of devices or quiet space to study, might be considered vulnerable and, therefore, able to attend full-time on-site provision.

Tier 3 local restrictions

2.12 The school will limit on-site attendance to just vulnerable students and children of critical workers, and year groups that the government identifies. All other students will receive remote education in line with section 3 of this appendix.

Tier 4 local restrictions

2.13 The school will limit on-site attendance to just vulnerable students. All other students will receive remote education in line with section 3 of this appendix.

3. Teaching and learning

3.1 The school will ensure staff and students follow the school's Online Safety Guidance when working and learning remotely.

3.2 All students will have access to high-quality education when learning remotely.

3.3 The school will prioritise factors that have been found to increase the effectiveness of remote education. These include, but are not limited to:

- Ensuring students receive clear explanations.
- Supporting growth in confidence with new material through scaffolded practice.
- Application of new knowledge or skills.
- Enabling students to receive feedback on how to progress.

3.4 The school will use a range of teaching methods to cater for all different learning styles, including:

PPT narration

Modelling using a visualiser

Videos

Reading and Comprehension exercises

Quizzes

Discussion

3.5 Teachers will ensure that a portion of their lessons are designed to promote interactivity amongst students and between students and staff, e.g. live lessons or use of the 'chat' function on meeting software, to lessen feelings of isolation and to promote student progress and motivation.

3.6 Teachers will ensure lessons are inclusive for all students and can be adapted to account for the needs of disadvantaged students and students with SEND.

3.7 When teaching students who are working remotely, teachers will:

- Set assignments so that students have meaningful and ambitious work each day.
- Deliver a planned, coherent and well-sequenced curriculum which allows skills to be built incrementally.
- Provide frequent, clear explanations of new content through high-quality curriculum resources, including through educational videos.
- Assess progress by using questions and other suitable tasks and be clear on how regularly work will be checked.
- Adjust the pace or difficulty of what is being taught in response to questions or assessments, including, where necessary, revising material or simplifying explanations to ensure students' understanding.
- Plan a programme that is of equivalent length to the core teaching students would receive in school, ideally including daily contact with teachers.

3.8 All provisions for remote learning will be subject to the class group's age, ability and/or any SEND.

3.9 In exceptional circumstances, the school may reduce its curriculum offering to enable students to cope with the workload – the Headteacher will assess this need, keeping students' best interests in mind, and will not take the decision lightly.

3.10 Teachers will continue to make use of formative assessments throughout the academic year, e.g. quizzes.

3.11 The school recognises that certain subjects are more difficult to teach remotely, e.g. music, sciences and physical education. Teachers will provide effective substitutes for in-person teaching such as video demonstrations.

3.12 Students will be encouraged to take regular physical exercise to maintain fitness, and time will be allocated within the school week for students to focus on this.

3.13 The school will remain cognisant of families who do not have access to the resources required for remote education, and will ensure that an up-to-date record of which students do not have appropriate devices or internet access is maintained.

3.14 The school will utilise the support available through the DfE's 'Get help with technology during coronavirus (COVID-19)' scheme.

3.15 Under the scheme, the school can order laptops, tablets and 4G wireless routers to support the following groups of students if they do not have access to a digital device or the internet through other means:

- Students in Years 3 to 11
- Clinically extremely vulnerable students across all year groups who are shielding or self-isolating in line with government advice
- Students in all year groups who are unable to access remote education whilst attending school on a hospital site

3.16 Before distributing devices, the school will ensure:

- The devices are set up to access remote education.
- Appropriate safeguarding controls and support are in place to help students use the devices safely.

3.17 Once devices are ready for collection, the school will either arrange for them to be collected by students or their parents from school, or delivered to students' homes, ensuring infection control measures are adhered to as part of this process.

3.18 The school will approach remote learning in a flexible manner where necessary, e.g. ensuring that lessons, live or otherwise, are recorded to accommodate contexts where students have to share a single device within the home.

3.19 Where live lessons are recorded, the school will ensure all recording procedures have due regard for the relevant data protection legislation, including the Data Protection Act 2018 and the General Data Protection Regulation.

3.20 The school will maintain good communication with parents to ensure that parents are aided in supporting their child's remote education.

4. Returning to school

4.1 The Headteacher will work with the LA to ensure students who have been learning remotely only return to school when it is safe for them to do so.

4.2 After a period of self-isolation, or the lessening of local restriction rules, the Headteacher will inform parents when their child will return to school.

4.3 The Headteacher will listen to all concerns that parents may have about their child returning to school and will advise them of the measures in place to ensure the safety of their child.

5. Monitoring and review

5.1 This policy annex will be reviewed in line with any updates to government guidance.

5.2 All changes to the policy will be communicated to relevant members of the school community.

APPENDIX C

ONLINE SAFETY GUIDANCE

The online world is a necessity for many children in accessing school work and it delivers huge benefits. However, there is always a risk online activity can leave children vulnerable. We have compiled the following support and guidance for parents and carers to guide loved ones when using online tools and support the digital life of the family.

Social Media Privacy Settings

There are age restrictions on the main social media websites. You need to make sure that your child stays away from these outlets until they have reached the age of consent ***AND*** until you are comfortable with him or her having an account. **Did you know that if a child lies about being 13 years of age when they are in fact only 10, when they reach 15 years of age their account status will state that they are 18?** This will mean when turning 15 the content filtering will be removed and they could be subject to inappropriate content. Some social media security settings are automatically lowered (Before the age of 18 there are friend-request restrictions to protect children)

- 13 years old: Facebook, Snapchat, Instagram, Tik Tok
- 16 years old: WhatsApp

If your children have downloaded common social media applications we recommend reviewing the privacy settings with your child on a regular basis. Mr Atkinson has created a series of videos to guide you through the process of checking these privacy settings on the most common applications. These can be found below:

Tik Tok Privacy Settings

https://youtu.be/lC1kdyyua-k

Snapchat Video

https://youtu.be/oWsjtKj3p7E

Instagram Video

https://youtu.be/-QxPFqGZKXE

Controlling Home Wi-Fi

The government has encouraged Internet Service Providers to support parents to easily filter content to put you in control of what your child can see online. You can switch on family friendly filters to help prevent age inappropriate content being accessed on devices in your home and the UK Safer Internet Centre provides guidance on how to do this for different internet service providers:

LINK FOR WEBSITE:

https://www.saferinternet.org.uk/advice-centre/parents-and-carers/parental-controls-offered-your-home-internet-provider

Advice for the Management of Devices

Create Ground Rules

If your children are old enough to be using the computer on their own, they are old enough to understand that there are rules they need to abide by. Breaking them should not have a lesser consequence than if they broke a rule in the offline world. The best way for families to agree on ground rules is to create a contract that all parties must sign.

Get To Know Who Your Child's 'Online Friends' Are

One of the contract rules should be that you have full access to your child's social media 'friends' and/or 'contacts' and that you can take a look whenever you wish.

Keep the devices in a Central Location

It's much easier to keep tabs on any online activity when the computer/tablet is located in a high-traffic zone than if your child is using a computer in the privacy of her own room. Place the computer/tablet in a central location like your kitchen or family room so that everything is out in the open.

Monitor the Pictures Your Child Posts Online

In an ideal world, your child would never post a photo of him/herself online, but that might not be entirely realistic. If he/she wants to share photos with her friends via email or a social media outlet, be sure you know exactly which pictures are being posted. Make sure the content of the photo is completely innocuous and that no identifiable locales in the background are noticeable. Your child should also NEVER post a picture of somebody else online unless they have asked permission to do so.

Be a Good Example of How to Use Social Media

If you are tweeting and updating your 'status' at a stop light and taking every opportunity to "just check something," you're setting a poor precedent for social media usage that your child will surely follow. Always remember to ask yourself if you're setting a good example and demonstrating proper technology etiquette as well.

Limit Device use

Just as you would limit use of a computer, TV or gaming system, you can do the same with a mobile phone. Set rules for the device, only allowing mobile phone usage at certain hours in the evening or after homework has been completed.

Teach Children about an Online Reputation – THINK BEFORE YOU POST
Many children don't seem to understand the permanence of the online world. Make sure to stress to your children what a digital footprint is and the impact inappropriate messages or images could have if a future college administrator or employer were to stumble upon them. Things posted online *STAY* online.

Talk to Children about Online Dangers
You may feel like you're scaring your children when talking to them about the dangers of being online, but it's better for them to be scared than to be unaware. Having an open line of communication is crucial the minute your children start using the Internet more independently.

Take control of your child's *geolocation*

Young people must be aware of who they are sharing their location with. If they are accessing a social networking site via a smartphone or mobile device, they might be disclosing their location without realising it. Location services can be turned on or off within the settings of a device.

What help is available if my child is being exploited online?

It is important to safeguard our loved ones from a range of online harms, whether that's child sexual exploitation, fraud, or extremist influences seeking to radicalise vulnerable people.

Online concerns can be reported directly to CEOP (Child Exploitation and Online Protection command)

https://www.ceop.police.uk/Safety-Centre/

If you are concerned that your child may be at risk of radicalisation, help is available through Prevent to make sure they get the support they need to move away from harmful influences. Contacting the authorities will not get the individual into trouble if a criminal act hasn't been committed. The local authority or police will discuss your concerns, suggest how they can best help and give you access to relevant support and advice.

https://www.gov.uk/report-terrorism

E-Safety Taught at Thornleigh

Within the Computer Science Curriculum students are taught an E-Safety unit of work at the start of every year, with a focus on highlighting key online dangers and dealing with online concerns.

Within the E-Safety unit of learning, Year 7 students are taught about:

-What personal data is and how to protect our online date.

-Online Friends and masquerading

-Privacy settings

-Digital Footprints and online reputation

-Reliability of information and data online (including phishing scams)

-How to report online concerns

-Cyber Bullying and its consequences

-Strong Passwords

Year 8 students are taught about:

- Digital Footprints
- Copyright and Creative Commons
- Password Control
- Cyber Security (including malware and online threats)
- Social Engineering
- Computer Misuse Act

All students take part in a yearly age-appropriate 'E-Safety week' in which students work within tutorial lessons to support them with a variety of different online concerns. This has included; online grooming and fake profiles, online reputations, sexting, online etiquette. Students are given the chance to check their social media privacy settings with trained experts.

Other useful websites:

As a parent, you can have a vital part to play in helping children stay safe online and we encourage you to have regular conversations with your children about online safety and their rights and responsibilities.

For detailed support with helping your child stay safe online and to initiate these conversations, we would encourage you to visit the following websites:

NSPCC website:

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Sexting

https://www.nspcc.org.uk/keeping-children-safe/online-safety/sexting-sending-nudes/

Reporting Abuse/Inappropriate Content:

https://www.thinkuknow.co.uk/

General Internet Support and Guidance:

https://www.internetmatters.org/advice/11-13/

APPENDIX D

ICT ACCEPTABLE USE FORM

1. Introduction

The purpose of this policy is to ensure that all users (including but not limited to Employees, Students, Visitors, Contractors) of Thornleigh Salesian College (referred to as 'the school') ICT facilities are aware of school policies relating to their use.

The school encourages the use of Information and Computing Technologies (referred to as 'ICT Facilities') for the benefit of its users. ICT Facilities are provided to support staff & students, specifically for educational, training, administrative or research purposes. This policy has been created to ensure a safe & secure ICT environment for all members of the school community.

It is the responsibility of all users of school ICT facilities to be aware of and follow school ICT policies and guidelines and to seek advice in case of suspected or apparent misuse.

Users are required to agree to the methods, practices and restrictions outlined within this policy before accessing school ICT Facilities, the prompt for which is displayed prior to logon on all school desktop PCs.

For ease of use, a simplified student agreement is supplied as an easy reference for everyday usage and disciplinary matters.

2. ICT Facilities

2.1 ICT facilities are managed by IT Support. Use of ICT facilities is at the discretion of the Senior Leadership Team (referred to as 'SLT'), and the Network Manager.

2.2 **Definitions**

2.2.1 The phrase 'ICT Facilities' as used in school policies should be interpreted broadly as including any ICT hardware (both desktop and portable), printers, telephones, or software/online services owned or operated by the school, including any allocation of storage on any local or cloud based school systems.

2.3 **Ownership**

2.3.1 ICT facilities owned by the school and software and/or data developed or created (for whatever reason) on that equipment remains in all respects property of the school. The Patents Act 1977 and Copyright, Design and Patents Act 1998 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

2.4 **End User Devices (Desktop PCs / Laptops / Mobile Devices)**

2.4.1 End User Devices are a critical asset to the school and must be managed carefully to maintain security, data integrity and efficiency.

2.4.2 IT Support has measures in place to prevent installation of software. Users should not attempt to install non-standard software on school devices. Any software installation requests must be submitted to IT Support.

2.4.3 All users have access to appropriate areas on the school's file servers for the secure storage of school /work related files.

2.4.4 Laptop & Mobile devices are at a high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that the hardware is stored securely both on and off site.

2.4.5 To protect the integrity of the school systems and data procedures, passwords or authentication devices for gaining remote access to the school systems must not be stored with the computer. This includes the saving of passwords into remote access software.

2.4.6 Confidential data is not be taken offsite via removable media / etc. Remote Access provides a secure Remote Desktop System that is encrypted and secure. If there is a requirement to take any confidential data offsite then please discuss with the Network Manager, to ensure the school's GDPR obligations as a Data Controller are met.

2.4.7 In event of loss or theft of a device you should report the matter promptly to the Director of School Services & the Network Manager. IT Support reserve the right to remotely locate, revoke access to and/or initiate a remote wipe of school managed devices or accounts.

2.5 **Loan Equipment**

2.5.1 The policy regarding loan equipment is similar to that for laptops and mobile devices. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment must complete an Equipment Loan Form, co-signed by a member of IT Support. The User then bears responsibility for the equipment detailed there-in. Loan equipment should be stored securely when not in use.

2.5.2 If loan equipment is lost or stolen the user responsible should report the matter promptly to IT Support to enable loss / theft procedures detailed in 2.4.7.

2.5.3 If loan equipment incurs damage, please inform the Network Manager – users should not attempt to fix or have the device repaired themselves. In the event of damage, repair / replacement charges may be applied at the discretion of Senior Leadership Team.

2.6 **ICT Disposal**

2.6.1 All ICT equipment is disposed of by IT Support using a WEEE certified disposal company. Disposal documentation is retained by IT Support. Under no circumstances may users dispose of equipment themselves.

2.7 **Software & Managed Services**

2.7.1 All software present on school Devices has been assessed and verified for use by IT Support. Users should not attempt to install non-standard software on school devices. IT Support has measures in place to prevent installation of software on school owned devices. If additional software is required a purchase and/or installation request must be submitted to IT Support via the Helpdesk.

2.7.2 All purchase orders for software should be submitted to IT Support prior to purchase to ensure compatibility and avoid duplication of services. The use of unverified or unauthorised software can cause unforeseen problems with school ICT facilities.

2.7.3 Mobile Apps loaded onto school owned mobile devices that are deemed 'on loan' are the responsibility of the user in terms of configuration and licensing unless otherwise agreed by IT Support. IT Support cannot guarantee support for apps purchased without prior consultation.

2.8 **Network Access & Data Storage**

2.8.1 In order to use the ICT facilities of the school a person must first be provided with their own unique User Account by IT Support. Access to ICT facilities implies, and is conditional upon, acceptance of this Acceptable Use Policy. Staff and Student user accounts are automatically generated when a record is added to the school MIS System. Accounts for additional systems and external managed services are generated and managed by IT Support unless otherwise stated.

2.8.2 All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. Passwords protect the school's systems from access by unauthorised people; they are for the protection of all school systems and data held within them. Users are personally responsible and accountable for all activities carried out under their user account. This applies to all school-based and externally hosted/externally managed services.

2.8.3 Passwords for personal user accounts must never be divulged to another person. If a password is forgotten or misplaced, a member of IT Support can assist in reset / recovery measures. Attempts to access, or use, any user account, which is not authorised to the user are strictly prohibited.

2.8.4 Passwords should be suitably complex so as not to be guessed easily. IT Support enforce basic password requirements on the school Network that reflect real-world practices found on most common websites and services. The requirements for the school Network and associated services are:

1. Passwords must be at least eight characters in length.

2. Passwords must contain characters from three of the following four categories:

i. Uppercase characters (A through Z)
ii. Lowercase characters (a through z)
iii. Digits (0 through 9)
iv. Special characters (for example, !, $, #, %)

3. Passwords must not contain the elements of the user's real name or account username eg. Their forename or surname.

2.8.5 Wi-Fi access for guests, staff and students is provided on a secure, segregated wireless network, access to which is at the discretion of Senior Leadership Team and IT Support. IT hardware/equipment not owned by the school may not be connected directly to the internal school network without prior written request and technical approval by IT Support.

2.8.6 It is school policy to store User Data on designated file servers. These servers are regularly backed up to secure recovery locations using industry standard backup software.

Users should store data appropriately dependent on its purpose and in accordance with relevant government legislation. User accounts are each allocated a secure 'My Documents' mapped drive along with appropriate access to secure network locations depending on their role within the school. It is each user's responsibility to store data appropriately. If you require further information regarding appropriate data storage please contact the Director of School Services or the Network Manager.

2.8.7 The School maintains a notification with the Information Commissioner's Office in compliance with the General Data Protection Regulation 2018. It is the responsibility of all school staff to ensure that personal data held and processed is within the terms of the school's data protection policy.

2.8.8 The school reserves the right to access any User Data held within ICT Facilities and/or externally hosted school systems when deemed appropriate by Senior Leadership.

2.8.9 Staff & Student Accounts are automatically disabled within 24 hours of the account holder being marked as 'Leaver' within the school MIS System. Secure User areas relating to leavers are securely retained as part of the school backup policy and in accordance with Data Protection Legislation.

2.8.10 Account access can be restored to users for limited periods when deemed appropriate by Senior Leadership / IT Support. If you require account access after officially leaving Thornleigh Salesian College please contact the Headteacher.

2.8.11 Storage space on the school network is finite. Secure User Areas (attached to all staff & student accounts in the form of 'My Documents') are for work and educational use only. Users should keep non-work related documents & files to a minimum. Users should not store any personal photos or videos on the network, nor should they use the school network to backup personal devices such as mobile

phones / tablets. Access to non-work related files can and will be removed without warning at the discretion of IT Support based on storage requirements. Please contact IT Support for current guidance on appropriate storage of personal files.

2.8.12 Due to storage limitations, quotas are enforced on all user areas. These quotes are designed to ensure the fair distribution of IT storage, taking into account the changing requirements of users. It is every user's responsibility to ensure unnecessary files do not use up valuable storage space. If you require additional storage space, please contact IT Support via the Helpdesk.

2.8.13 Although it is not policy to routinely examine the content of individual user areas, the school reserves the right to monitor user areas at any time, for specific instances in which there is good cause for such monitoring or legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee/student wrongdoing, protect the rights or property of the school, to protect the school ICT system security, to obtain essential business information after reasonable efforts have been made to contact the user or to comply with legal process.

2.9 **Wireless Access & Remote Access**

2.9.1 The school currently provides wireless facilities for all school owned mobile devices, staff owned mobile devices and where appropriate guest owned devices. All wireless access is provided at the discretion of IT Support and can be removed / revoked at any time.

2.9.2 Secure Wi-Fi access is provided for TSC staff members using the 'TSC Staff' Wi-Fi network (SSID). Staff may access this network using their school network username & password. Access to this network is strictly for staff-owned devices only, IT Support reserve the right to revoke device access at any time. Network access is monitored in real-time by IT Support.

2.9.3 Secure Wi-Fi access is provided for Sixth Form Students using the 'Thornleigh Sixth Form' Wi-Fi network (SSID). Sixth Form students may access the network using their school network username & password. Access to this network is strictly for Thornleigh Sixth Form student-owned devices. Further details of usage and restrictions of this network can be found in the Student IT Agreement document.

2.9.4 By connecting to the school Wi-Fi, users are agreeing to the terms of this document and any additional agreement required prior to connection. It is the responsibility of the individual to ensure their device software/OS is up-to-date, free from viruses and any other malicious software. IT Support reserves the right to revoke network access for any device deemed a threat to network security.

2.9.5 Designated users may access files and applications via the school's remote access facility. This is provided via a secure Remote Desktop System.

2.9.6 Access to the school Remote Desktop System is provided to all staff and select students at the discretion of IT Support & Senior Leadership Team. IT Support reserve the right to remove access to the Remote Desktop System without prior

notice when deemed necessary by the Headteacher on the advice from the Network Manager.

3. Data Security

3.1.1 Users must only access data held on the school's computer systems if they have been properly authorised to do so. Said data should only be used in the context of performed their designated role.

3.2 **Personal Data and the General Data Protection Regulation (GDPR)**

3.2.1 The school maintains a notification with the Information Commissioner's Office in compliance with the General Data Protection Regulation (GDPR). It is the responsibility of all school staff to ensure that personal data held and processed is within the terms of the school's data protection policy.

3.2.2 Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons.

3.2.3 The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

3.4 **Anti-Virus / Anti-Spam Protection**

3.4.1 Sophos Enterprise Anti-virus software is installed on all domain computers as standard and is updated regularly. Users are not permitted to disable or interfere with the running of anti-virus software.

3.4.2 Non-school software or data files intended to be run on school equipment by persons other than staff or students (including by not limited to school guests & contractors) must be checked for viruses before use. If you suspect that a virus has infected school ICT facilities immediately cease use and contact IT Support.

3.4.3 Un-encrypted files received by or sent by e-mail are checked for viruses automatically. Encrypted files may not always be scanned depending on their contents and file type. It is the user's responsibility to avoid accessing any suspect files and if received to alert IT Support to their presence.

3.4.4 Remote users are responsible for maintaining up to date anti-virus software on their own computers. Please contact IT Support if you require advice on protecting your personal device.

3.4.5 All user & email accounts provided to staff & students are the property of the school and are designed to assist in the process of teaching & learning. Users should have no expectation of privacy in any email sent or received, whether it is of a business or personal nature.

4. E-Mail

4.1 **Use and Responsibility**

4.1.1 Staff - the school email system is provided for the school's business purposes and academic support. Limited personal use of the email system is permitted, but not to a level that would influence the primary business purpose. The school will be held liable for any contractual arrangements entered into by email by members of staff if it is reasonable for the recipient to assume that such people are acting with authority (employer's vicarious liability). Such commitments should be avoided unless specifically authorised.

4.1.2 Students - the school's email system is provided to aid users with their studies. Personal use of the email system is permitted, but the account is only valid whilst you are a student at the school.

4.1.3 Users should not use school email when purchasing personal goods.

4.1.4 The email system costs the school time and money to maintain. It should be used judiciously in the same manner as other school resources such as telephones and photocopying.

4.1.5 School-wide email messages must be business related and of significant importance to all employees. Non-school email accounts should not be used for conducting school business unless in an emergency situation.

4.2 **Content**

4.2.1 Email messages must be treated like any other formal written communication. Improper statements in email can give rise to personal liability and liability for the school and can constitute a serious disciplinary matter.

4.2.2 Email messages to or from a school email address cannot be considered to be private or confidential to the individual.

4.2.3 Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

4.2.4 Confidential or sensitive information should always be encrypted before being sent via email.

4.2.5 Thornleigh Salesian College email servers operate TLS 1.2 (Transport Layer Security) to ensure email is secured against interception when passing outside of the college network.

4.2.6 Additional message-level email encryption is utilised by TSC senior leadership & administrative staff in the form of Egress Protect. Staff are required to use Egress Protect when sending sensitive data of any form via email to third parties outside of the school network. Recipient sign-up is required to use the service. If you are unsure about the use or application of Egress Protect please contact IT Support. Further information on Egress is available at https://supportcentre.egress.com

4.2.7 Email messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability are strictly prohibited. It is never permissible to subject another person to public humiliation or ridicule; this is equally true via email. Any user found to have broken the above statute may have access to their school email account revoked without notice which may result in action via the school's Disciplinary Procedure.

4.2.8 Copyright law applies to email. Do not use e-mail to transmit or circulate copyrighted materials.

4.3 **Privacy**

4.3.1 Email messages to or from a school email address cannot be considered to be private or confidential. School emails will be regarded as the joint property of the school and the individual staff member or student.

4.3.2 Although it is not policy to routinely examine the content of individual emails, the school reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee/student wrongdoing, protect the rights or property of the school, to protect the school ICT system security, to obtain essential business information after reasonable efforts have been made to contact the mailbox user or to comply with legal process.

4.3.3 Emails are routinely scanned for the use of offensive language, inappropriate content/attachments, data protection breaches & spam content.

4.3.4 Messages sent or received may be copied and disclosed by the school for lawful purposes without prior notice. Requests for access/monitoring unless required by law will only be authorized by a member of SLT.

4.3.5 It is not permissible to access or to send email from another users account either directly or indirectly, unless directed to do so by Senior Leadership Team in the performance of your stated job role.

5. Internet

5.1 **Internet**

5.1.1 All Internet usage from the school network is monitored and logged. Reporting on aggregate usage is performed on a regular basis. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an investigation may result in action via the school's Disciplinary Procedure and possibly criminal investigation.

5.1.2 Copyright and licensing conditions must be observed when downloading material or content from the internet or moving material on and off school network storage.

5.1.3 Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites.

5.1.4 The school reserves the right to remove access to any site(s) which it feels may inhibit the primary business purpose of school.

5.1.5 The use of Social Media and its inherent dangers is outlined in the school Social Media Policy.

6. Private use, legislation and updates to this policy

6.1 **Private Use**

6.1.1 ICT facilities are provided for the school's business and educational purposes and responsible personal use is therefore allowed provided there is no conflict with the interest or requirements of the school.

6.1.2 The school does not accept liability for any personal loss or damage incurred through using the ICT facilities for private use.

6.2 **Legislation**

6.2.1 The following are a list of Acts that apply to the use of the school's ICT facilities:

- Regulation of Investigatory Powers Act 2000
- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- General Data Protection Regulation 2018
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights Act 1998

6.3 **Updates to this Policy**

6.3.1 In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available. This policy will be reviewed annually.

Student IT Agreement – AUP supplemental

Students are permitted to use Thornleigh Salesian College ICT Facilities after agreeing to the following conditions:

1. I will use school ICT facilities, including the internet, e-mail, digital video, mobile devices, 3rd party services etc. for school purposes only.

2. I will not download or attempt to install software on school ICT Facilities.

3. I will only access the school network and 3rd party services using my own username and password supplied to me by the school.

4. I will follow the school's ICT Acceptable Use Policy and not reveal my passwords to anyone and change them regularly.

5. I will only use my school e-mail address on school ICT facilities.

6. I will make sure that all ICT communications with other students, teachers or others are responsible and sensible.

7. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

8. 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.

9. 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 them into disrepute.

10. 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

11. I will respect the privacy and ownership of others' work on-line at all times.

12. I will not attempt to bypass the school internet filtering system in any way, regardless of what device I am using.

13. I understand that all my use of school ICT Facilities including Internet access and other related technologies is monitored and logged and can be made available on request to teachers.

14. I understand that these rules are designed to keep me safe and that if they are not followed, college sanctions will be applied and my parent/carer will be contacted.

Signature _____

Printed Name _____

Date _____

APPENDIX E

ICT EQUIPMENT LOAN FORM

Date of Loan: …….

Proposed Date of Return: …….

Name of Student ……

Equipment: ……
(incl Serial Number)

……..…

The ICT equipment listed above is the property of Thornleigh Salesian College and has been loaned to you for a period agreed with the Headteacher. After this time, the equipment must be returned to school, complete and in good working order. If the equipment is lost, damaged or has parts missing then you may be liable for the cost of either replacement, parts or other repairs.

I agree with the terms and requirements

Signed …… Date ……
Student

Signed …….. Date ……
Parent / Carer

Signed …… Date ……
Representative of Thornleigh Salesian College

Item Returned on: ……..…….

Signature of Parent/Student: ……

Signature of Staff Member: ……