ONLINE SAFETY POLICY

SENIOR SCHOOL, JUNIOR SCHOOL AND NURSERY (INCLUDING EYFS)

Authorised by	Deputy Head (Pastoral)
Date	November 2024
Date of next review	November 2025 or earlier as required

1 Scope

1.1 The School is committed to promoting and safeguarding the welfare of all pupils and an effective online safety strategy is paramount to this.

1.2 The aims of the School's online safety strategy are threefold:

1.2.1 to protect the whole School community from illegal, inappropriate and harmful content or contact;

1.2.2 to educate the whole School community about their access to and use of technology; and

1.2.3 to establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

1.3 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications Technology (collectively referred to in this policy as **Technology**). Examples of technologies covered by this policy include, but are not limited to, websites, email, instant messaging, blogging, social networking sites, chat rooms, media downloads, gaming sites, text and picture messaging, video calls, podcasting, online communities, mobile devices, cloud technologies, virtual and augmented reality, artificial intelligence and online learning platforms.

1.4 This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's Technology whether on or off School premises, or otherwise use Technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

1.5 Both this policy, and the School's Acceptable Use policies, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

1.6 In designing this policy, the School has considered the "4Cs" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the School recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the School's behaviour policies and/or Safeguarding and Child Protection Policy and Procedures as is appropriate in the circumstances.

1.7 The following policies, procedures and resource materials are also relevant to the School's online safety practices:

1.7.1 Junior School Acceptable use policy for pupils;

1.7.2 Senior School Acceptable use policy for pupils;

1.7.3 Staff IT acceptable use policy and social media policy;

1.7.4 Child Protection and Safeguarding Policy and Procedures;

1.7.5 Senior School Anti-bullying policy;

1.7.6 Junior School Anti-bullying policy;

1.7.7 Risk assessment policy for pupil welfare;

1.7.8 Staff code of conduct (including use of mobile phones and cameras in the EYFS setting) and whistleblowing policy;

1.7.9 Data protection policy for staff; and

1.7.10 Information security policy (including remote working and bring your own device to work).

1.7.11 Junior School Online safety Guidance (see Appendix 1)

1.7.12 Relationship and Sex Education Policy (Senior School)

1.7.13 Relationships Education, Sex Education and Health Education Policy including PSHE (Personal, Social, Health and Economic Education) (Junior School & Nursery)

1.7.14 Behaviour, Rewards and Sanctions Policy (Senior School)

1.7.15 Culture and Ethos Policy (Junior School & Nursery)

1.7.16 AI Policy (Senior School)

1.8 These policies, procedures and resource materials are available to staff on the School's intranet and hard copies are available on request.

1.9 This is a whole school policy and applies to all sections of Churcher's College, including the Senior School, Junior School and Nursery (including Early Years Foundation Stage). Throughout this policy document, the terms 'the School' and 'Churcher's College' refer to all sections of Churcher's College, unless otherwise specified.

2 Roles and responsibilities

2.1 The Governing Body

2.1.1 The Governing Body as proprietor has overall responsibility for safeguarding arrangements within the School, including the School's approach to online safety and the use of Technology within the School.

2.1.2 The Governing Body is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Governing Body's response to this duty.

2.1.3 The Designated Safeguarding Governor is the senior board level lead with leadership responsibility for the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Governing Body. In addition, there is a nominated Online safety Governor.

2.1.4 The Governing Body will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in paragraph 1.2 above.

2.2 **Headmaster and Senior Management Team**

2.2.1 The Headmaster has overall executive responsibility for the safety and welfare of members of the School community.

2.2.2 The Designated Safeguarding Lead is the senior member of staff from the School's leadership team with lead responsibility for safeguarding and child protection. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Child Protection and Safeguarding Policy and Procedures.

2.2.3 The Designated Safeguarding Lead will work with the Director of Digital Systems, the Deputy Head (Academic) and the Junior School Online Safety Co-ordinator (see below) in monitoring Technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

2.2.4 **Junior School and Nursery (including EYFS):** the Deputy Head of the Junior School is the Junior School Online Safety Co-ordinator and, together with the Senior Teacher (Academic), takes day to day responsibility for online safety issues. The Senior Teacher (Academic) is a member of the School's Digital Strategy Group, which is responsible for issues relating to online safety and monitoring the online safety policy.

2.2.5 **Senior School:** The Deputy Head (Pastoral)/Designated Safeguarding Lead is the Senior School Online Safety Co-ordinator and takes day to day responsibility for online safety issues. The Deputy Head (Pastoral)/Designated Safeguarding Lead is a member of the School's Digital Strategy Group, which is chaired by the Deputy Head (Academic). The Digital Strategy Group is responsible for issues relating to online safety and monitoring the online safety policy. The Digital Strategy Group works in consultation with the whole Senior School community including the Digital Leaders IT Committee, which is comprised of a number of pupils across the age range.

2.2.6 The Designated Safeguarding Lead will regularly monitor the Senior School Technology Incident Log, which he maintains in conjunction with the Director of Digital Systems and the Deputy Head (Academic), and the Junior School Technology Incident Log, which is maintained by the Deputy Head and Senior Teacher (Academic) in the Junior School.

2.2.7 The Designated Safeguarding Lead will regularly update other members of the School's Senior Management Team on the operation of the School's safeguarding arrangements, including online safety practices.

2.3 **Director of Digital Systems**

2.3.1 The Director of Digital Systems, together with his team, is responsible for the effective operation of the School's filtering and monitoring systems so that pupils

and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

2.3.2 The Director of Digital Systems is responsible for ensuring that:

(a) the School's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

(b) the user may only use the School's Technology if they are properly authenticated and authorised;

(c) the School has effective filtering and monitoring policies in place, which are applied and updated on a regular basis;

(d) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;

(e) the use of the School's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(f) monitoring software and systems are kept up to date to allow the IT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

2.3.4 The Director of Digital Systems will report regularly to the Health, Safety and Welfare Committee, which is chaired by the Headmaster, on the operation of the School's Technology. The Senior Management Team is represented on the Health, Safety and Welfare Committee, which is attended by the nominated Governor for Health and Safety. If the Director of Digital Systems has concerns about the functionality, effectiveness, suitability or use of Technology within the School, including of the monitoring and filtering systems in place, he will escalate those concerns promptly to the appropriate members(s) of the School's Senior Management Team.

2.3.5 **Senior School:** The Director of Digital Systems, the Deputy Head (Pastoral)/Designated Safeguarding Lead and the Deputy Head (Academic) are responsible for maintaining the Senior School Technology Incident Log (a central record of all serious incidents involving the use of Technology) and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's Child Protection and Safeguarding Policy and Procedures.

2.3.6 **Junior School and Nursery (including EYFS):** The Junior School Deputy Head and Senior Teacher (Academic) are responsible for maintaining the Junior School Technology Incident Log (a central record of all serious incidents involving the use of Technology) and bringing any matters of safeguarding concern to the attention of the Head or Deputy Head of the Junior School (Deputy Designated Safeguarding Leads) who will liaise with the Designated Safeguarding Lead as appropriate in accordance with the School's Child Protection and Safeguarding Policy and Procedures.

2.4 **All staff**

2.4.1 All staff have a responsibility to act as good role models in their use of Technology and to share their knowledge of the School's policies and of safe practice with the pupils.

2.4.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in paragraph 1.7 above.

2.4.3 Staff are responsible for promoting and supporting safe behaviours in their classrooms. When pupils use School IT or Technology whilst in the care of the School, staff should ensure that supervision is appropriate for the pupils involved.

2.4.4 Staff should raise any concerns about online safety with the Deputy Head (Pastoral) in the Senior School or the Deputy Head in the Junior School & Nursery.

2.4.5 All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases, abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

2.4.6 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Child Protection and Safeguarding Policy and Procedures. **In all cases, if staff are unsure, they should always speak to the DSL (or a Deputy).**

2.5 **Parents**

2.5.1 The role of parents in ensuring that pupils understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:

(a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

2.5.2 If parents have any concerns or require any information about online safety, they should contact the Deputy Head (Pastoral) in the Senior School and the Deputy Head of the Junior School in the Junior School and Nursery. They can also consult the online safety resources detailed in paragraph 4.3.3 and, in the Senior School, the online safety news and advice page on My School Portal.

3 Filtering and Monitoring

3.1 Churcher's College aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

3.2 Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour, Rewards and Sanctions Policy (or the Culture and Ethos Policy in the Junior School), as appropriate.

3.3 The school's filtering system blocks internet access to harmful sites and inappropriate content. If there is a good educational reason why a particular website, application, or form of content should not be blocked, a pupil should submit a request to the IT Helpdesk, including an explanation as to why temporary access is required, the area of the curriculum to which it relates and the relevant member of the teaching staff. The IT Helpdesk, following consultation with the relevant member of staff, will notify the pupil of the School's decision. Any unblocking will be for a duration specified by the IT Helpdesk and pupils must comply with the provisions of all relevant school policies (including this policy and the IT Acceptable Use Policy) when accessing the unblocked material.

3.4 The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals be identified. The Director of Digital Systems will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately.

Staff:

3.5 If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content.

3.6 While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the IT Helpdesk if they believe that appropriate teaching materials are being blocked.

Pupils:

3.7 Pupils must report any accidental access to inappropriate material to the appropriate teacher. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour, Rewards and Sanctions Policy (Culture and Ethos Policy in the Junior School). Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

3.8 Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work/research purposes, pupils should contact the IT Helpdesk for assistance.

4 Education and training

4.1 Pupils

4.1.1 The safe use of Technology is integral to the School's ICT curriculum eg as part of the KS1, KS2 and KS3 Computing and PSHE programmes of study. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices (see the School's Curriculum Policies).

4.1.2 Technology is included in the educational programmes followed in the EYFS in the following ways:

(a) children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

(b) children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

(c) children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

4.1.3 The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies, PSHE and tutorial / pastoral activities, teaching pupils:

(a) about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;

(b) to be critically aware of content they access online and guided to validate accuracy of information;

(c) how to recognise suspicious, bullying or extremist behaviour;

(d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

(e) relevant laws applicable to the internet;

(f) the consequences of negative online behaviour; and

(g) how to report cyberbullying (including the CEOP button on Firefly) and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

4.1.4 The safe use of Technology aspects of the curriculum are reviewed on a regular basis to ensure their relevance.

4.1.5 The School's acceptable use policies for pupils set out the School rules about the use of Technology including internet, email, social media and mobile electronic devices,

helping pupils to protect themselves and others when using Technology. Pupils are reminded of the importance of these policies on a regular basis.

4.1.6 **Useful online safety resources for pupils**

http://www.thinkuknow.co.uk/

http://www.childnet.com/young-people

https://www.saferinternet.org.uk/advice-centre/young-people

http://www.safetynetkids.org.uk/

https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

4.2 **Staff**

4.2.1 The School provides training on the safe use of Technology to staff so that they are aware of how to protect pupils and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.

4.2.2 Induction training for new staff includes training on the School's online safety strategy including this policy, the Staff Code of Conduct, Staff IT Acceptable Use Policy and Social Media Policy. Ongoing staff development training includes training on Technology safety together with specific safeguarding issues including sexting, cyberbullying and radicalisation.

4.2.3 Staff also receive data protection training on induction and at regular intervals afterwards.

4.2.4 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

4.2.5 **Useful online safety resources for staff**

https://swgfl.org.uk/education-tech/

https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

http://www.childnet.com/teachers-and-professionals

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

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

http://educateagainsthate.com/

https://www.commonsense.org/education/

DfE's Advice for head teachers and school staff on cyberbullying

DfE's Advice on the use of social media for online radicalisation

DfE's guidance Teaching online safety in schools, updated January 2023

UKCCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people, December 2020

UKCCIS Online safety in schools and colleges: Questions from the Governing Board

College of Policing Briefing Note: Police action in response to youth produced sexual imagery

Professionals Online Safety Helpline: helpline@saferinternet.org.uk, 0344 381 4772

Education for a connected world framework (UKCCIS)

Internet Watch Foundation – an internet hotline for the public and IT professionals to report potentially criminal online content

https://www.digitalawarenessuk.com/

4.3 **Parents**

4.3.1 The School works closely with parents to ensure they can safeguard their children whilst using Technology. The Senior School aims to run an annual online safety seminar for parents, which is traditionally delivered by a representative from CEOP (the Child Exploitation and Online Protection command). On occasion, the School will communicate with parents on an ad hoc basis, for example in response to an incident involving a particular year group or when a specific issue is brought to the School's attention by an external agency such as the police. Relevant policies and resources are available to parents electronically on the Senior School Firefly Parent Portal. In the Junior School an anti-bullying booklet which includes information about cyberbullying is signed by parents and pupils at the start of each academic year.

4.3.2 Parents are encouraged to read the relevant acceptable use policy for pupils with their son / daughter to ensure that it is fully understood. The Senior School acceptable use policy is available to parents on Firefly.

4.3.3 **Useful online safety resources for parents**

https://www.saferinternet.org.uk/advice-centre/parents-and-carers

http://www.childnet.com/parents-and-carers

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

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

http://parentinfo.org/

http://parentzone.org.uk/

https://www.internetmatters.org/

DfE's Advice for parents and carers on cyberbullying

https://www.commonsensemedia.org/

https://www.askaboutgames.com/

https://www.ceop.police.uk/safety-centre/

UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019)

https://www.digitalawarenessuk.com/

5 Access to the School's Technology

5.1 The School provides internet and intranet access and an email system to pupils and staff as well as other Technology. Pupils and staff must comply with the respective acceptable use policy when using School Technology. All such use is monitored by the IT team.

5.2 Pupils and staff require individual user names and passwords to access the School's internet, intranet and email system which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their user name or password must report it to the IT Helpdesk immediately.

5.3 No laptop or other mobile electronic device may be connected to the School network without the consent of the Director of Digital Systems. All computer systems must have updated, active antivirus software running. The use of any device connected to the School's network will be logged and monitored by the IT team.

5.4 The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored appropriately by the IT team.

5.5 **Use of mobile electronic devices**

5.5.1 The School has appropriate filtering and monitoring systems in place to protect pupils using the Internet (including email and social media sites) when connected to the School's network and their effectiveness is regularly reviewed.

5.5.2 Mobile devices equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet. Since the School cannot put adequate protection for the pupils in place, pupils are discouraged from using their mobile devices to connect to the Internet including accessing email or social media sites when in the School's care. In certain circumstances, a pupil may be given permission to use their own mobile device to connect to the Internet using the School's network. Permission to do so must be sought and given in advance.

5.5.3 The School rules about the use of mobile electronic devices are set out in the relevant acceptable use policy for pupils and also, in the case of the Senior School, in the School Rules and Information.

5.5.4 The school rules relating to mobile phones are as follows:

CCJS&N: Pupils are not permitted to bring mobile phones (or watches with camera, videoing or messaging capabilities) into school.

Senior School:

(a) 1st to 5th Year pupils are permitted to bring mobile phones to school but these must be switched off and placed securely in a Yondr pouch between 8.30am and 4pm.

(b) Sixth Form students are permitted to bring mobile phones to school and may use their devices in the social areas of the Ramshill Sixth Form Centre and in workrooms (provided that this does not impact on the studies of another student). Sixth Form students are not permitted to use mobile phones outside of Ramshill or in front of younger pupils.

5.5.5 The use of mobile electronic devices by staff is covered in the code of conduct, IT acceptable use policy, social media policy, data protection policy for staff and information security policy (including remote working and bring your own device to work).

5.5.6 The School's policies apply to the use of Technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

6 Procedures for dealing with incidents of misuse

6.1 Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

6.2 **Misuse by pupils**

6.2.1 Anyone who has any concern about the misuse of Technology by pupils should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the relevant anti-bullying policy where there is an allegation of cyberbullying.

6.2.2 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Child Protection and Safeguarding Policy and Procedures).

6.3 **Misuse by staff**

6.3.1 Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's whistleblowing policy so that it can be dealt with in accordance with the staff disciplinary procedures.

6.3.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they should report it immediately in accordance with the School's procedures for reporting and dealing with allegations of abuse against staff set out in the School's Child Protection and Safeguarding Policy and Procedures.

6.4 **Misuse by any user**

6.4.1 Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the Director of Digital Systems and / or the Designated Safeguarding Lead.

6.4.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

6.4.3 If the School considers that any person is vulnerable to radicalisation the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

7 Monitoring and review

7.1 **Senior School:** All serious incidents involving the use of Technology will be logged centrally in the Senior School Technology Incident Log by the Director of Digital Systems, Deputy Head (Pastoral)/Designated Safeguarding Lead and/or Deputy Head (Academic).

7.2 **Junior School and Nursery (including EYFS):** All serious incidents involving the use of Technology will be logged centrally in the Junior School Technology Incident Log by the Junior School Deputy Head and/or Senior Teacher (Academic).

7.3 The Designated Safeguarding Lead has responsibility for the implementation and review of this policy. The Designated Safeguarding Lead will consider the views of pupils and parents together with the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures and to consider whether existing security and online safety practices within the School are adequate.

7.4 Consideration of the effectiveness of the School's online safety procedures and the education of pupils about keeping safe online will be included in the Governors' annual review of safeguarding.

Appendix 1

Churcher's College Junior School and Nursery

Online Safety Guidance

Introduction

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

Computing 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 computing 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
- Email 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 computing, 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 Churcher's College Junior School we understand the responsibility to educate our pupils in online safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc).

Online safety information for parents

- Parents are asked to read through and sign the Acceptable Use Agreement on behalf of their child. Pupils will sign an acceptable use policy from Year 3 upwards.

- Parents are required to make a decision as to whether they consent to images of their child being taken and used for publicity
- The school will send out relevant online safety information through newsletters, schools COMS, the school website, on Firefly and on Seesaw.

Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach online safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils in Reception to Year 5 are not allowed to bring personal mobile devices/phones to school. Any devices/phones that are brought to school will be sent to the school office and kept there until the end of the day.
- Pupils in Year 6 are not allowed to bring phones to school but they are invited, but not obliged, to bring in one device (either laptop, Chromebook or iPad) for use in lessons, to assist with their learning. Children are not permitted to browse the world wide web or social media without the permission of the teacher in charge.
- In the case of all pupils, the sending of abusive or inappropriate text messages outside school is forbidden.

Managing video-conferencing

- When it is introduced into our school, videoconferencing will be appropriately supervised for all pupils' age.

Use of staffs' personal equipment

- Staff working in the Early Years Foundation Stage should not use their own personal mobile phones, cameras or other electronic devices with imaging and sharing capabilities whilst working with the children to photograph or record the pupils. The Early Years Foundation Stage class teacher will monitor use of equipment in the classroom and make all staff aware of this protocol. Photographs of pupils will only be taken by approved individuals in agreement with the Early Years Foundation Stage class teacher and images will only be used for school purposes.
- When working in school mobile phones should be "on silent". Unless it is an emergency staff should not use phones for communication during their working hours. Phone calls and texts should be sent during breaks and non- contact periods only.

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils (from Year 3) must sign up to the Acceptable Use Agreement for pupils and abide by the school's online safety rules. These online safety rules will also be displayed clearly in all classrooms.

- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's online safety rules and within the constraints detailed in the school's online safety policy.

- All staff must read the Computing Policies, Protocol and Procedures before using any school ICT resource.

Password Security

- Users are provided with an individual network, email username and password, which they are encouraged to change periodically.

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

Communications Policy

Introducing the online safety policy to pupils

- Online safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by the Head of Computing every year and at relevant points throughout e.g. during PSHCE lessons/circle times/anti-bullying week/ Safer Internet Day.
- Pupils will be informed that network and Internet use will be monitored**.**

Online safety on social media for parents

The purpose of this policy is to:

- Encourage social networking sites to be used in a beneficial and positive way by parents (not pupils as they are below the age of 13)
- Safeguard pupils, staff and anyone associated with the school from the negative effects of social networking site
- Safeguard the reputation of the school from unwarranted abuse on social networking sites
- Clarify what the school considers to be appropriate and inappropriate use of social networking sites by parents
- Set out the procedures the school will follow where it is considered that parents have inappropriately or unlawfully used social networking sites to the detriment of the school, staff, pupils or anyone else associated with the school

The school uses Facebook to engage with its parental community on an informal and day-to-day basis. Social media websites have occasionally been used to fuel campaigns and complaints against schools, school staff, and in some cases other parents/pupils. Churcher's College considers the use of social media websites being used in this way as unacceptable and not in the best interests of the children or the whole school community. Any concerns parents may have about the school or their child must be made through the appropriate channels. Please see the School's Complaints Policy for further details.

In the use of social media there are certain considerations that the school has catered for. The parental permission slip regarding the use of children's photographs for marketing applies to Facebook and other social media platforms. Images are made more difficult to access because the usual ability to 'right click' and 'save as' has been disabled. The school understands that it is impossible to fully secure any photograph when published anywhere on the web.

The Facebook wall is monitored by the school for interaction and it is the schools position that the Wall is not the area for communications regarding individual children. The Facebook wall is configured to not allow posting of photographs or videos by parents. It has a profanity filter set to

'high' in place though there is no reason to expect issues from inappropriate content from parents; these are precautionary measures only.

In the event that any pupil or parent/carer of a child/ren being educated at Churcher's College is found to be posting libellous or defamatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this. The school will also expect that any parent/carer or pupil removes such comments immediately. School will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step the school will usually discuss the matter with the parent to try and resolve it and to ask that the relevant information be removed from the social networking site in question.
In serious cases the school will also consider its legal options to deal with any such misuse of social networking and other sites.

Additionally, and perhaps more importantly, is the issue of cyber bullying and the use by any member of the school community to publicly humiliate another by inappropriate social network entry. We will take and deal with this as a serious incident of school bullying.

Monitoring and review
This guidance is implemented on a day-to-day basis by all Junior School and Nursery staff and is monitored by the Junior School Online Safety Coordinator.

The Junior School online safety guidance will be revised by the Junior School Online Safety Coordinator.