St Benedict's Catholic College

Online Safety Policy

Date Reviewed	November 2020
Staff Consultation	October 2017
Date of next Review	November 2023

1. *Aims and policy scope*

1.1 St Benedict's Catholic College believes that online safety is an essential element of safeguarding young people and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

1.2 St Benedict's Catholic College realises that the internet and information communication technologies are an important part of everyday life, so young people must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

1.3 St Benedict's Catholic College has a duty to provide our community with quality internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

1.4 St Benedict's Catholic College realises that there is a clear duty to ensure that all young people and staff are protected from potential harm online.

1.5 The purpose of our online safety policy is to:

- Clearly identify the key expectations of all members of the community with regards to the safe and responsible use of technology to ensure that St Benedict's' Catholic College is a safe and secure environment.
- Safeguard and protect all members of our community online.
- Raise awareness with all members of our community regarding the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

1.6 This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the college (collectively referred to as 'staff' in this policy) as well as young people and parents/carers.

1.7 This policy applies to all access to the internet and use of information communication devices, including personal devices, or where young people, staff or other individuals have been provided with college issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2. Key responsibilities for the community

2.1 The key responsibilities for the senior leadership team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the college community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect young people from inappropriate content which meet the needs of the college community whilst ensuring young people have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of college systems and networks and to ensure that the college network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

- Ensuring that online safety is embedded within a progressive whole college curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Ensuring there are robust reporting channels for the college community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Governing Body is identified with a lead responsibility for Safeguarding, including supporting online safety.

2.2 The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the college lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the college's safeguarding recording structures and mechanisms.
- Monitor the college online safety incidents to identify gaps/trends and use this data to update the college's education response to reflect need.
- To report to the college senior leadership team, Governing Body and other agencies as appropriate, on online safety concerns.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with the college senior leadership team to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis with stakeholder input.
- Ensuring that online safety is integrated with other appropriate college policies and procedures.

2.3 The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the college Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of college systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the young people in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following college safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.

2.4 The key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.

- Taking responsibility for the implementation of safe security of systems and data in partnership with the senior leadership team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on college-owned devices.
- Ensuring that the college's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the college's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and senior leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and senior leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the college's IT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all college machines and portable devices.

2.5 The key responsibilities of young people are:

- Reading the college Acceptable Use Policy (AUP) and adhering to it.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Using college systems, such as learning platforms, and other network resources, safely and appropriately.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

2.6 The key responsibilities of parents and carers are:

- Reading the college Acceptable Use Policy and Statement of Partnership, encouraging their child to adhere to it, and adhering to it themselves where appropriate.
- Discussing online safety issues with their child, supporting the college in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the college, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

3. ***Online Communication and Safer Use of Technology***

3.1 Managing the college website

- The college will ensure that information posted on the college website meets the requirements as identified by the Department for Education (DfE).
- Email addresses will be published carefully online, to avoid being harvested for spam

3.2 Publishing images and videos online

- Written permission from parents or carers will always be obtained before images/videos of students are published. This consent may be withdrawn by the parent.

3.3 Managing email

- Students may only use college provided email accounts for educational purposes.
- All members of staff are provided with a specific college email address to use for any official communication.
- The use of personal email addresses by staff for any official college business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to college email systems will always take place in accordance with data protection legislation
- Members of the community must immediately tell the IT support team if they receive offensive communication
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and students and parents.
- Excessive social email use can interfere with teaching and learning and will be restricted. Access in college to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending.
- College email addresses will not be used for setting up personal social media accounts.
- Care will be taken to ensure that any reply is sent **only** to relevant people and that "email chains" are not inadvertently sent with the reply.

3.4 Appropriate and safe classroom use of the internet and any associated devices

- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- All members of staff are aware that they cannot rely on filtering alone to safeguard young people and supervision, classroom management and education about safe and responsible use is essential.
- Students will be appropriately supervised when using technology, according to their ability and understanding.
- All college owned devices will be used in accordance with the college Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The college will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledges the source of information.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a college requirement across the curriculum.

- The college will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.

3.5 Management of college learning platforms

- Students/staff will be advised about acceptable conduct and use when using learning platforms.
- Only members of the current student, parent/carers and staff community will have access to learning platforms.
- All users will be mindful of copyright issues and will only upload appropriate content onto learning platforms.
- When staff, students' etc. leave the college their account or rights to specific college areas will be disabled.

4. ***Social Media Policy***

4.1 ***General social media use***

- Expectations regarding safe and responsible use of social media will apply to all members of college community and exist in order to safeguard both the college and the wider community, on and offline.
- All members of St Benedict's Catholic College will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the college community.
- All members of St Benedict's Catholic College are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The college will control student and staff access to social media and social networking sites whilst on site and when using college provided devices and systems
- The use of social networking applications during college hours for personal use is not permitted,
- Any concerns regarding the online conduct of any member of St Benedict's Catholic College on social media sites should be reported to the senior leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour, staff disciplinary and safeguarding/child protection.
- Any breaches of college policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour, staff disciplinary and safeguarding/child protection.

4.2 Official use of social media

- Official use of social media sites by the college will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be formally approved by the Principal.
- Official college social media channels will be set up as distinct and dedicated social media sites or accounts for educational or engagement purposes.
- Staff will use college provided email addresses to register for and manage any official approved social media channels.
- A copy of the username and password for the account will be kept in the college safe.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.

- Any online publication on official social media sites will comply with legal requirements.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Written permission from parents or carers will always be obtained before images/videos of students are published. This consent may be withdrawn.
- Links to official social media use will be published through the College newsletter.
- Official social media channels will link back to the college website to demonstrate that the account is official.
- The college will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

4.3 Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the college Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current students or past students who are under 18, via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead.
- All communication between staff and members of the college community on college business will take place via official approved communication channels (such as an official college provided email address or phone numbers)
- Staff will not use personal social media accounts to make contact with students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Principal.
- Any communication from students/parents received on personal social media accounts will be reported to the college's designated safeguarding lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with college's policies and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

- Members of staff will notify the senior leadership team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the college.
- Members of staff are encouraged not to identify themselves as employees of St Benedict's Catholic College on their personal social networking accounts. This is to prevent information on these sites from being linked with the college and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the college on social media.
- Members of staff who follow/like the college social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

4.4 ***Students use of social media***

- Safe and responsible use of social media sites will be outlined for young people and their parents as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to students as part of the curriculum.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, college attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and secure passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with students and written parental consent will be obtained, as required.
- The college is aware that many popular social media sites state that they are not for young people under the age of 13, therefore the college will not create accounts within college specifically for young people under this age.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at college, will be dealt with in accordance with existing college policies including anti-bullying and behaviour.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at college, will be raised with parents/carers, particularly when concerning any underage use of social media sites

5. Use of Personal Devices and Mobile Phones

5.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among young people, young people and adults will require all members of the college community to ensure that mobile phones and personal devices are used responsibly.
- We recognise that personal communication through mobile technologies is an accepted part of everyday life for young people, staff and parents/carers but requires that such technologies need to be used safely and appropriately within college, in accordance with the college mobile phone policy.

5.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate college policies
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The college accepts no responsibility for the loss, theft or damage of such items. Nor will the college accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content by any member of the community via mobile phones or personal devices is forbidden and any breaches will be dealt with as part of the discipline/behaviour policy.
- All members of the college community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the college community will be advised to use appropriate security to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen.
- All members of the college community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the college policies.

5.3 Students use of personal devices and mobile phones

- All use of mobile phones and personal devices by young people will take place in accordance with the Acceptable Use Policy.
- Students' personal mobile phones and personal devices will be switched off and kept out of sight during lessons and while moving between lessons.
- Mobile phones or personal devices will not be used by students during lessons or formal college time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- If a student needs to contact their parents/carers they will be allowed to use a college phone or their personal mobile phone under staff supervision.
- Parents are advised not to contact their child via their mobile phone during the college day, but to contact the college office.
- Students should protect their phone numbers by only giving them to trusted friends and family members.
- Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student breaches the college policy then the phone or device will be confiscated and will be held in a secure place in the Sanctuary. Mobile phones and devices will be released to parents/carers in accordance with the mobile phone policy.

5.4 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting young people or their families within or outside of the college in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with their line manager.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of young people unless they are running an official social media channel.
- Staff will not use any personal devices directly with young people and will only use work-provided equipment during lessons/educational activities. Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant college policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched to 'silent' mode during lesson times.

- Bluetooth or other forms of communication should be “hidden” or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless prior permission has been given by a member of the senior leadership team
- Staff will ensure that any content brought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or to have committed a criminal offence then the police will be contacted.

6. ***Use of the internet***

6.1 St Benedict’s Catholic College is aware that the internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

6.2 Emerging technologies will be examined for educational benefit and the college leadership team will ensure that appropriate risk assessments are carried out before use in college is allowed.

6.3 The college will ensure that appropriate filtering and monitoring systems are in place to prevent staff and students from accessing unsuitable or illegal content.

6.4 The college will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a college computer or device.

6.5 The college will provide an Acceptable Use Policy for any guest/visitor who needs to access the college computer system or internet on site.

6.6 All staff, students and visitors will read and sign the Acceptable Use Policy before using any college resources.

6.7 Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability.

6.8 Parents will be asked to read the Acceptable Use Policy for student access and discuss it with their child.

6.9 When considering access for vulnerable members of the community (such as with young people with special education needs) the college will make decisions based on the specific needs and understanding of the student(s).

6.10 An online safety curriculum will be established and embedded throughout the whole college, to raise awareness regarding the importance of safe and responsible internet use amongst students, covering both safe college and home use. The college will ensure that this is differentiated, with input from specialist staff as appropriate.

6.11 Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.

6.12 All members of staff will be made aware that their online conduct out of college could have an impact on their role and reputation within college. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.13 The college recognises that parents/carers have an essential role to play in enabling young people to become safe and responsible users of the internet and digital technology.

6.14 Parents’ attention will be drawn to the college online safety policy and expectations in newsletters, letters, college prospectus and on the college website.

6.15 Parents will be encouraged to role model positive behaviour for their children online.

6.16 Filtering and Monitoring

- All users will be informed that use of college systems will be monitored and that all monitoring will be in line with legislation.
- The college uses Smoothwall filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The college has a clear procedure for reporting breaches of filtering.
- If staff or students discover unsuitable sites, the URL will be reported to the IT support team and will then be recorded and escalated as appropriate.

- Changes to the college filtering policy will be risk assessed by IT support staff prior to any changes.
- The college will undertake regular checks to ensure that the filtering methods selected are effective and appropriate.
- Any material that the college believes is illegal will be reported to appropriate agencies immediately

7. ***Management Information Systems***

7.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection legislation.

7.2 The security of the college information systems and users will be reviewed regularly.

7.3 Personal data sent over the internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.

7.4 Portable media containing college data must be encrypted

7.5 Unapproved software will not be allowed in work areas or attached to email.

7.6 All staff users will be expected to log off or lock their screens/devices if systems are unattended.

7.7 The college will log and record internet use on all devices attached to the college network

7.8 Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- All users must always keep their password private and must not share it with others or leave it where others can find it.
- All users are required to use STRONG passwords for access into our system.
- All users are required to change their passwords every term

7.9 Apps/systems which store personal data will be risk assessed prior to use.

7.10 Online / Cloud systems

- Uploading of information to cloud based learning systems is shared between different staff members according to their responsibilities.
- Use of cloud systems other than those for which accounts are provided by the IT support team must be agreed in advance by the college's Data Protection Officer.
- Photographs and videos uploaded to the cloud systems must only be accessible by members of the college community.

8. Remote Learning

8.1 Teaching online is different to teaching face-to-face. Staff will only use platforms that have been approved by the college and will always maintain professional relationships with children and young people.

8.2 Video-conferencing programs should not be used on a one-to-one basis between staff and students– remote learning on a one-to-one basis is not appropriate

8.3 During online activity staff and students will be in a neutral area, (ie, not in a bedroom or bathroom) and wearing appropriate clothing

8.4 Staff and students will only use college allocated email addresses, not personal ones, or use usernames and passwords which must not be shared with others

8.5 Students' personal information such as their location, date of birth or phone number should be kept private

9. Responding to Online Incidents and Safeguarding Concerns

9.1 All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and within the curriculum for students.

9.2 All members of the college community must report online safety concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc to the designated safeguarding lead or the IT Support team as appropriate.

9.3 Any reported incidents will be dealt with using the established college procedures, maintaining confidentiality where appropriate.
9.4 After any investigations are completed, the college will debrief, identify lessons learnt and implement any changes as required.
9.5 Where necessary, follow up action may be taken using the student behaviour policy or the staff disciplinary policy as appropriate.

10. Related reading

This policy must be read in conjunction with other relevant college policies including (but not limited to)

- safeguarding and child protection policies
- anti-bullying policy
- behaviour policy
- whistleblowing policy
- Personal Social and Health Education (PSHE) Policy
- Sex and Relationships Education (SRE) Policy

Appendix A - Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding child protection / sexualisation

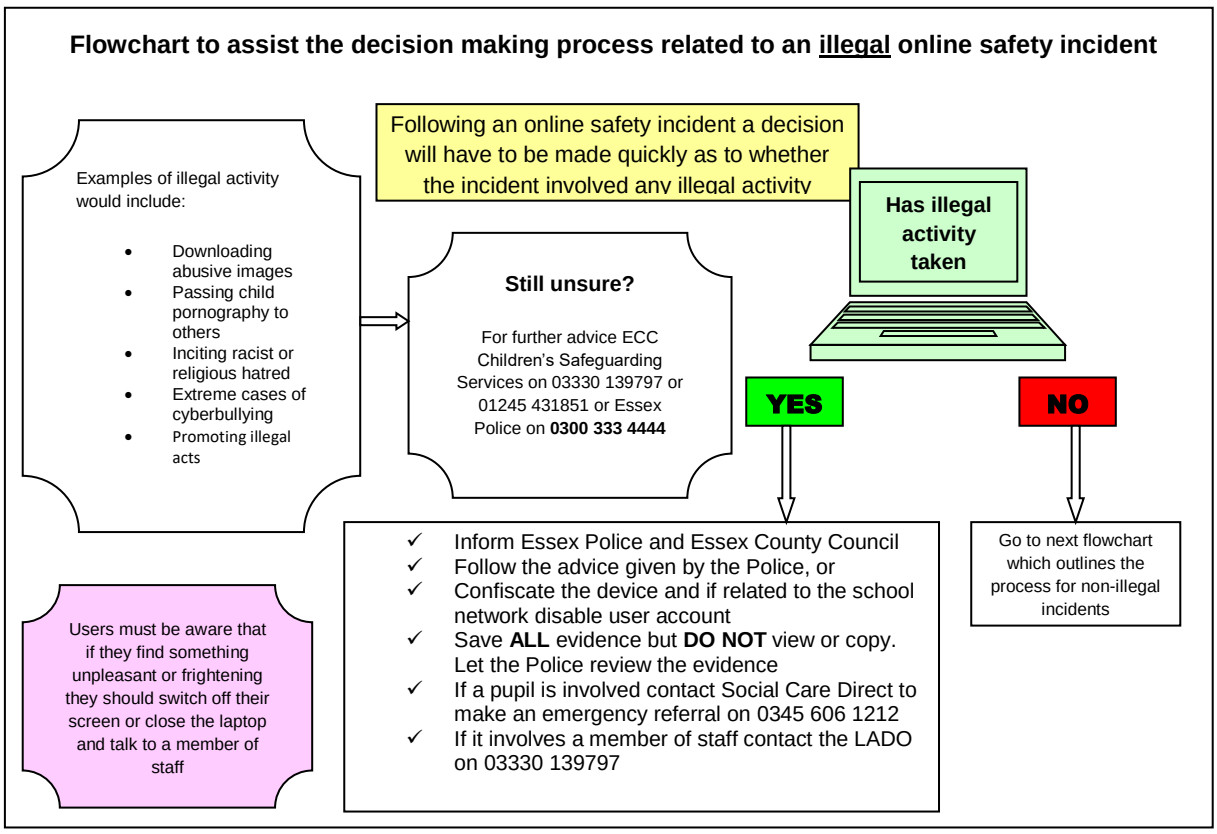
- The SET Procedures will be followed.

Responding to concerns regarding online hate, radicalisation and extremism online

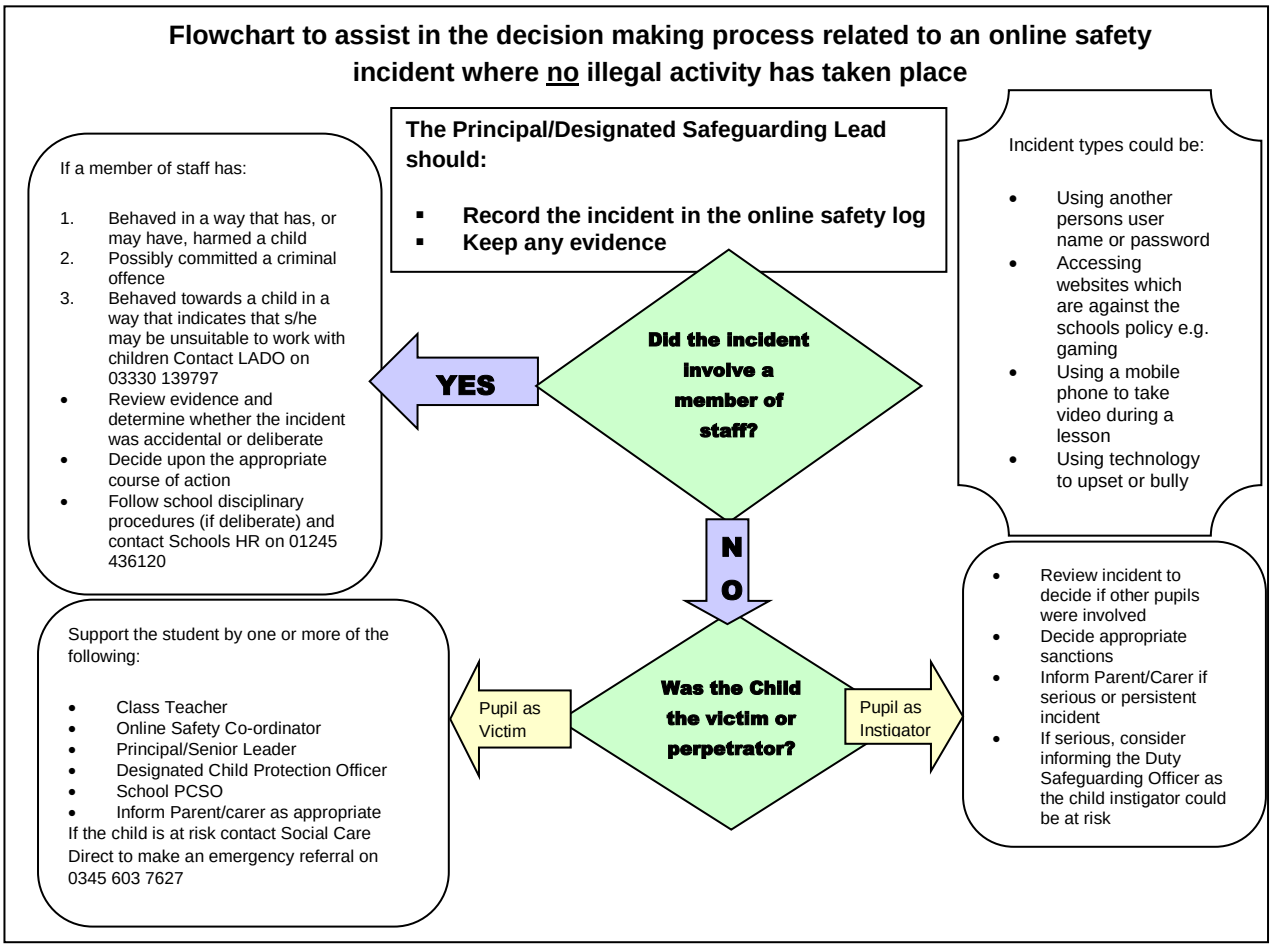
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing college policies, including anti-bullying, behaviour etc.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy and Prevent strategy.

Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the college community will not be tolerated. Full details are set out in the college policies and response regarding anti-bullying and behaviour.



Flowchart to assist in the decision making process related to an online safety incident where no illegal activity has taken place



Appendix B – Student AUP

Responsibility

- I know I must respect the college's systems and equipment and if I cannot act responsibly then I will lose the right to use them
- I will only use IT systems in college, including the internet, e-mail, digital video, mobile technologies, etc. for college purposes
- I will not download or install software on college IT equipment
- I know that online content might not always be true

Privacy

- I will keep my password and personal information private
- I will only log on to the college network / cloud storage (Office 365) with my own user name and password
- I know I must always check my privacy settings are safe and private

Communication

- I will only use my college e-mail address for college related communication
- I will make sure that all IT communications with students, teachers or others are responsible and sensible
- I will only take / use images of students and/or staff for college purposes

Respect and Reputation

- I will always think before I post as once I upload text, photos or videos they can become public and impossible to delete
- I will not use technology to be unkind to people

Safe and Legal

- I know that my internet use is monitored to protect me and ensure I comply with the college's acceptable use policy
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a college project approved by my teacher
- I am aware that copyright laws exist and I need to ask permission before using other people's content and acknowledge any sources I use
- I know it can be a criminal offence to hack accounts or systems or send threatening and offensive messages
- I know my online actions have offline consequences

Report

- I know that people online aren't always who they say they are and that I must always talk to an adult before meeting any online contacts
- If anything happens online which makes me feel worried or uncomfortable then I will speak to an adult I trust and visit www.thinkuknow.co.uk

Sample letter

Dear Parent/Carer

IT including the internet, learning platforms, e-mail and mobile technologies continue to be an important part of learning at St Benedict's College. We expect all students to be safe and responsible when using IT at the college. It is essential that students are aware of online safety and know how to stay safe when using IT. Information about staying safe online is taught in computing lessons and can be found on the college website at https://www.stbenedicts.essex.sch.uk/safeguarding

Students are asked to read and discuss the attached agreement with their parent or carer and then to sign and follow the terms of the agreement while at the college. Any concerns or explanation can be discussed with their class teacher or any member of the leadership team at the college.

The college uses a range of online systems, including learning resources such as MathsWatch, which store limited student details. Full information about these systems can be found in the privacy notice section of our website.

Please return the bottom section of this form to the college for filing by DATE. Failure to return the form below may result in removal of IT privileges.

Yours faithfully

Mrs J E Santinelli
Principal

✂----------

To: College office by DATE

Student and parent/carer signature

Name of student: ..... Form: .....

I have discussed this document with my parent/carer and I agree to follow the online safety rules and to support the safe and responsible use of IT at St Benedict's College.

Student signature…….

I have discussed this document with my child and I will encourage them to follow the online safety rules and to support the safe and responsible use of IT at St Benedict's College.

Parent/Carer signature ……..…….

Date ……

Appendix C – Staff / Governor AUP

IT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in college. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents. All members of the college community are expected to use ICT responsibly and comply with applicable laws and with normal standards of professionalism. Any concerns or clarification should be discussed with the Principal or appointed representative.

1. I will only use the college's e-mail / internet / intranet / cloud storage (Office 365) and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Governing Body.
2. I will comply with the IT system security and not disclose any passwords used for services provided to me by the college or other related authorities. I will not share my passwords with others.
3. I will ensure that all electronic communications with students and staff are compatible with my professional role, and take place through official college channels.
4. I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to students.
5. I will only use the approved, secure e-mail system(s) for any college business, ensuring that the content is appropriate, accurate and data protection compliant.
6. I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in college, taken off the college premises or accessed remotely. Personal data can only be taken out of college or accessed remotely when authorised by the Principal or Governing Body.
7. I will not install any hardware or software on college owned equipment without permission of the business manager or a member of the college IT technical team.
8. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
9. Images of students and/or staff will only be taken, stored and used for professional purposes in line with the college Online Safety (formerly eSafety) policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the college network without the permission of the parent / carer, member of staff and the Principal.
10. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Principal. I understand that the college respects my privacy and will not routinely do this.
11. I will respect copyright and intellectual property rights.
12. I will ensure that my online activity, both in college and outside college, will not bring the college or my professional role into disrepute.
13. I will support and promote the college's Online Safety (formerly eSafety) policy and help students to be safe and responsible in their use of IT and related technologies.
14. If required, I will complete an additional staff AUP – if I am running official social media channels on behalf of the college

Bring Your Own Device Guidance

Our AUP (overleaf) states that:

I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in college, taken off the college premises or accessed remotely. Personal data can only be taken out of college or accessed remotely when authorised by the Principal or Governing Body.

Please see the clarifications below:

1. Any memory sticks or portable hard disks used MUST be encrypted
2. Any data taken out of college MUST be copied only to an encrypted memory stick or hard drive – the use of other removable media is not permitted
3. Data must not be uploaded to any storage site except the college provided Office 356 One Drive
4. Data used out of college MUST be accessed remotely or stored on an encrypted hard drive or memory stick. It must not be saved on personal machine hard drives (please note this includes laptops)
5. Use of college email on shared computers MUST be via Office 365 Outlook Web Access. The password MUST not be saved to the device.
6. Use of college email on mobile devices (phones/tablets) is permitted in the following circumstances
    a. The device is encrypted with biometric security (finger or facial recognition) or a 6 digit pin. A finger pattern is not acceptable
    b. If the device is used by others, (eg your child), the email application/browser window is closed before the device is given to them and they are instructed not to open it. If available, the email application MUST be protected with a separate password
    c. Any loss/theft/replacement/repair of the device is reported to the college, so email data can be securely wiped remotely
    d. Any device must be securely wiped before sold/given away/handed-down
    e. At the request of the Principal, the college reserves the right to remotely wipe any device connected to our Office 365 server

The college makes a remote desktop service available. The use of this is preferable to the use of data on personal devices.

Notes:

1. Teacher markbooks should not contain sensitive personal data such as medical, SEN, Pupil Premium etc., unless these are held electronically and securely.
2. Care must be taken to ensure that sensitive personal data is NEVER displayed on a projection screen.
3. Data must not be uploaded to any website without express permission from the Business Manager.

User Signature
I agree to follow this acceptable use agreement and to support the safe and secure use of IT throughout the college.

Signature ……..... **Date** ……
Full Name ……..... (printed) **Job title** …….....

Appendix D – 7 top tips for keeping young people safe online

1. Keep being a TEAM

It's important to work together as a family to help keep your kids safe online. That's why we've created four simple steps so you Talk, Explore, Agree and Manage online safety.

Talk to your child regularly about what they're doing online and how to stay safe. Let them know they can come to you, another trusted adult or **Childline** if they're feeling worried or upset by anything they've seen.
Explore your child's online activities together. Understand why they like using certain apps or games and make sure they know what they can do to keep themselves safe.
Agree your own online rules as a family.
Manage your technology and use the settings available to keep your child safe.

2. It's ok to be flexible

The internet is playing a really important role for children and families, whether it's for chatting, gaming, schooling, or even exercising.

It's ok to be flexible, but make sure you talk to your child about any new rules and remind them they can talk to you about anything they see or do online. Create a **family agreement** together Family agreements are designed to be flexible to your family's needs so it's important to update them when situations change.

3. Talk to them about who they're talking to

The online world has helped us keep in touch with family and friends we haven't been able to see this year. But sometimes kids might talk to people they don't know online, like on games or social media sites.

Make sure you're chatting regularly to your child about who they're talking to online and what apps they're using. Remind them that they shouldn't share any personal information, like names, locations or links to other social media sites. Tell them if someone starts asking them questions or suggests using another app like **Snapchat** or **Instagram** they should come and tell you.

Explore safety settings together like block and report so your child knows how to stop unwanted contact or end an online chat if it's not about the game.

It can be helpful to supervise children when they're online but it can also be time consuming! If your child is chatting or playing with friends online, you could always talk to other parents and see if you can take it in turns to supervise and support them, just like you would if they were at each other's houses.

4. Get familiar with video chatting and livestreaming

Do you know the difference between video chatting, video sharing and livestreaming? Don't worry if the answer is no, it can be confusing (especially when some apps do more than one!)

5. Take online safety offline

To help you keep your kids safe, we've created some activity sheets to make it even easier for you to have conversations about staying safe online.

6) Get to know gaming

Playing games online can be a great way for kids to be creative, learn new skills and stay connected with friends over lockdown. But with so many different games available, and new ones popping up all the time, it can be difficult to stay on top of what your child is doing.

Familiarise yourself with your child's favourite game and use our reviews to help you decide whether it's appropriate for them to use. Look out for things like the age rating and whether it has any chat features.

Before you let your child use a new game, agree some rules around who they can play with and when.

7. Think about age and content ratings

If your child is using new apps or playing popular games, it can be hard to know if they're age-appropriate or not. To make it more confusing, there's often an official, app store and PEGI rating, which is sometimes based on age and other times on content

Appendix E - Online Safety (e-Safety) Contacts and References

Action Fraud: www.actionfraud.police.uk

Anti Bullying Alliance: www.anti-bullyingalliance.org.uk

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Essex Safeguarding Children Board: https://www.escb.co.uk/

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

National Online Safety: https://nationalonlinesafety.com/

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety and www.net-aware.org.uk/

Online Compass: http://www.onlinecompass.org.uk/

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

SWFfL: https://swgfl.org.uk/ – Southwest Grid for Learning promote safe and secure use of the Internet

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

UK Council for Internet Safety: www.gov.uk/government/organisations/uk-council-for-internet-safety

360 Safe Self-Review tool: https://360safe.org.uk/