Bennett Memorial Diocesan School

Online Safety Policy

Approval Arrangements

All statutory policies in the Trust are ultimately the responsibility of the Trust Board. To enable it to discharge this responsibility appropriately and in collaboration with the constituent schools, the Trust Board will:

1. set a full Trust wide policy,
2. set a ‘policy principles’ document (a framework within which Headteachers develop a full and appropriately customised policy),
3. or delegate to Headteachers or LGBs the power to develop their own policy.

This is a Level 2 Policy against the Trust Governance Plan.

Review Body:	**LGB**	**Review Period:**	**1 year**
Approved:	**September 2023**	**Next review:**	**September 2024**

This policy was approved by the LGB for implementation on the date above and supersedes any previous Online Safety policy.

This policy has been written in accordance with:
KCSIE September 2023
Working Together to Safeguard Children July 2018

1. Online Safety

- It is essential that children are safeguarded from potentially harmful and inappropriate material or behaviour online. Bennett Memorial Diocesan School adopts a whole school approach to online safety which will empower, protect, and educate our students and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

- Bennett Memorial Diocesan School will ensure online safety is reflected as required in all relevant policies. Online safety is considered as a running and interrelated theme when devising and implementing our policies and procedures and when planning our curriculum, staff training, the role and responsibilities of the DSL and parental engagement.

- Bennett Memorial Diocesan School identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

  - *Content*: being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
  - *Contact*: being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
  - *Conduct*: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
  - *Commerce*: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

- Bennett Memorial Diocesan School recognises that technology, and the risks and harms related to it, evolve and change rapidly. The school will carry out an annual review of our approaches to online safety, supported by an annual risk assessment which considers and reflects the risks our children face.

- The headteacher will be informed of online safety concerns by the DSL, as appropriate. The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

- Please see the separate policy for online safety that can be found on the school website.

1.1 Policies and Procedures

- The DSL has overall responsibility for online safety within the school but will liaise with other members of staff, for example IT technicians, curriculum leads etc. as necessary.

- The DSL will respond to online safety concerns reported in line with our child protection and other associated policies, including our anti-bullying, staff code of conduct and behaviour policies.

  - Internal sanctions and/or support will be implemented as appropriate.
  - Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

- Bennett Memorial Diocesan School uses a wide range of technology. This includes computers, laptops, tablets and other digital devices, the internet, our learning platform, intranet and email systems.

  - All school owned devices and systems will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

- Bennett Memorial Diocesan School recognises the specific risks that can be posed by mobile and smart technology, including mobile/smart phones, cameras and wearable technology. In accordance with KCSIE 2022 Bennett Memorial Diocesan School has appropriate mobile and smart technology and image use procedures in place, which are shared and understood by all members of the community. See acceptable use policies.

1.2 Appropriate Filtering and Monitoring

- Bennett Memorial Diocesan School will do all we reasonably can to limit children's exposure to online harms through school provided devices and networks and in line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place. We currently operate the Smoothwall Filtering system.

    - Our leadership team and relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
    - All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation
    - Filtering breaches or concerns identified through our monitoring approaches will be recorded and reported to the DSL who will respond as appropriate
    - Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the Internet Watch Foundation and the police
    - Students will use appropriate search tools, apps and online resources as identified following an informed risk assessment
    - Students internet use will be supervised by staff according to their age and ability
    - Students will be directed to use age appropriate online resources and tools by staff

- When implementing appropriate filtering and monitoring, Bennett Memorial Diocesan School will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

- Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety and we recognise that we cannot rely on filtering and monitoring alone to safeguard our pupils; effective safeguarding practice, robust policies, appropriate classroom/behaviour management and regular education/training about safe and responsible use is essential and expected.

    - Pupils will use appropriate search tools, apps and online resources as identified by staff, following an informed risk assessment.
    - Internet use will be supervised by staff as appropriate to pupils age, ability and potential risk of harm.

1.3 Responsibilities

- Our Trust Board and Trust executive leadership team has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the school leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

- The DSL is responsible for ensuring that our Bennett Memorial Diocesan School has met the DfE Filtering and monitoring standards for schools and colleges.

- The School senior leadership team are responsible for:

    - procuring filtering and monitoring systems.
    - documenting decisions on what is blocked or allowed and why.
    - reviewing the effectiveness of our provision.
    - overseeing reports.
    - ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
    - ensuring the DSL and school's IT Manager/staff have sufficient time and support to manage their filtering and monitoring responsibilities.

- The DSL has lead responsibility for overseeing and acting on:

    - any filtering and monitoring reports.
    - any child protection or safeguarding concerns identified.
    - checks to filtering and monitoring system.

- The school's IT Manager/staff have technical responsibility for:

    - maintaining filtering and monitoring systems.
    - providing filtering and monitoring reports.
    - completing technical actions identified following any concerns or checks to systems.
    - working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews and carry out checks.

- All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.

- All staff, pupils and parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

1.4 Decision making and reviewing our filtering and monitoring provision

- When procuring and/or making decisions about our filtering and monitoring provision, our senior leadership team works closely with the DSL and the school's IT Manager/staff. Decisions have been recorded and informed by an approach which ensures our systems meet our school specific needs and circumstances, including but not limited to our pupil risk profile and specific technology use.

- Any changes to the filtering and monitoring approaches will be assessed by staff with safeguarding, educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

- Our school undertakes an at least annual review of our filtering and monitoring systems to ensure we understand the changing needs and potential risks posed to our community.

- In addition, our school undertakes regular checks on our filtering and monitoring systems, which are logged and recorded, to ensure our approaches are effective and can provide assurance to the Trust Board and Trust executive leadership team that we are meeting our safeguarding obligations. These checks are achieved by:

    - IT Support Staff complete weekly checks and more frequently if required. This is informed by the content of the reports raised by Smoothwall.
    - Termly review with DSL and IT Manager to allow the DSL to review record keeping and to carry out a test on the filtering systems.

1.5 Appropriate filtering

- Bennett Memorial School's education broadband connectivity is provided through Cantium and it uses the Smoothwall filtering system].
  - Cantium is a member of Internet Watch Foundation (IWF).
  - Smoothwall are signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
  - Smoothwall blocks access to illegal content including child sexual abuse material (CSAM).
  - Smoothwall blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material. Please note this list is not exhaustive.

- We filter internet use on all school owned, or provided, internet enabled devices and networks. This is achieved by:
  - The default filtering system set through Smoothwall for Secondary Schools.
  - The school has the ability to change/edit the policy & access to fit around the schools current needs to prevent filtering inhibiting studies.
  - All such changes are logged
  - The Headteacher would have to approve a major filtering change via Cantium.

- Our filtering system is operational, up to date and is applied to all users, including guest accounts, all school owned devices and networks, and all devices using the school broadband connection. **This is checked on a daily basis by Cantium and the School IT Technical Department.**

- We work with Smoothwall and Cantium and our IT Manager/staff to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

- If there is failure in the software or abuse of the system, for example if pupils or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to turn off monitor/screen and report the concern immediately to a member of staff or report the URL of the site to the IT staff.

- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and behaviour policies.

- Parents/carers will be informed of filtering breaches involving their child.

- Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), Kent Police, NCA-CEOP or Kent Integrated Children's Services.

- If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or leadership team.

1.6 Appropriate monitoring

- We will appropriately monitor internet use on all school provided devices and networks. This is achieved by:
  - Students only being able to connect their devices via the BYOD WI-FI. The access level is set to primary school. We take their device MAC address which allows the IT Technical Team and Smoothwall to track their internet usage and filters accordingly.
  - Onsite devices are set to a standard student level but can be edited to give further access to help with the current curriculum requirements.
  - Staff have to adhere to the same process as students when using BYOD devices but the access level is set to staff access and limited to two devices per person.

- All users will be informed that use of our devices and networks can/will be monitored and that all monitoring is in line with data protection, human rights and privacy legislation. Further details can be found in the acceptable use agreement.

- If a concern is identified via our monitoring approaches:
  - Where the concern relates to pupils, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour policies.
  - Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the headteacher), in line with our staff behaviour/ allegations policy.

- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, Kent Police via 101, NCA-CEOP , LADO or Kent Integrated Children's Services.

1.7 Information security and access management

- Bennett Memorial Diocesan School is responsible for ensuring that appropriate security protection procedures are in place, in order to safeguard our systems as well as staff and students. Further information can be found in the online safety policy on the school website.

- Bennett Memorial Diocesan School is part of the Janet Network in Kent. Internet access passes through many firewalls before we access the internet. Part of these firewalls is the Smoothwall filter system. This is supplied to Bennett by EIS Kent. We have access to block and set filtering rules for staff and students.

- All students and staff members sign an acceptable use contract. Students are not allowed to use mobile telephones or wearable smart technology etc. during the school day.

- Bennett Memorial Diocesan School will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

- The Headteacher is responsible for ensuring that the school has met the DfE cyber security standards for schools and colleges. **The school is working towards meeting the cyber security standards certification.**

1.8 Remote / Online learning

- Bennett Memorial Diocesan School will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.

- All communication with students and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and/or agreed systems e.g., MS Teams
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL
- Staff and students will engage with remote teaching and learning in line with existing behaviour principles as set out in our school behaviour policy/code of conduct and Acceptable Use Policies.
- Staff and students will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

1.9 Online Safety Training for Staff

- Bennett Memorial Diocesan School will ensure that all staff receive online safety training, which, amongst other things, will include providing them with an understanding of the expectations, applicable roles and their responsibilities in relation to filtering and monitoring, as part of induction.
- Ongoing online safety training and updates for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach. See section 7 for more information.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- The DSL Nicola Santaana, and deputies Vicki Woosey, Jenny Hartland, Hannah Johnson and Lee Stoodley will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.

1.10 Educating Pupils

- Bennett Memorial Diocesan School will ensure a comprehensive whole school curriculum response is in place to enable all students to learn about and manage online risks effectively as part of providing a broad and balanced curriculum. See section 9 for more information.
- Students will be taught about online safety as part of the curriculum.
    - In **Key Stage 3**, students will be taught to:
        - Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
        - Recognise inappropriate content, contact and conduct, and know how to report concerns

- Students in **Key Stage 4** will be taught:
  - To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
  - How to report a range of concerns
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the IT services company, who provide our filtering service, can accept liability for the material accessed, or any consequences of internet access. The school will audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate.

1.11 Working with Parents/Carers

- Bennett Memorial Diocesan School will build a partnership approach to online safety and will support parents/carers to become aware and alert of the potential online benefits and risks for children by:

  - Providing information on our school website
  - Offering specific online safety events for parents
  - Writing to parents as required

- Bennett Memorial Diocesan School will ensure parents and carers understand what systems are used to filter and monitor their children's online use at school, what their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child is going to be interacting with online. This is achieved by providing information on our school website and policies such as acceptable use, home/school agreements and through existing communication channels. In addition, we are members of the National College and share relevant online safety resources that they produce regularly.

- Where the School is made aware of any potentially harmful risks, challenges and/or hoaxes circulating online, national or locally, we will respond in line with the DfE 'Harmful online challenges and online hoaxes' guidance to ensure we adopt a proportional and helpful response. Additional local advice and support is available via the Education Safeguarding Service and the ' Think before you scare' blog post.

1.12 Cyber Bullying

- Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

- Cyber bullying may include online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:

  - Non-consensual sharing of sexual images and videos
  - Sexualised online bullying
  - Unwanted sexual comments and messages, including on social media
  - Sexual exploitation; coercion and threats; and
  - Upskirting

1.13 Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

- The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training. The school also provides information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

1.14 Examining Electronic Devices

- School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

- When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

    - Cause harm, and/or
    - Disrupt teaching, and/or
    - Break any of the school rules

- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

    - Delete that material, or
    - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
    - Report it to the police

- Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Students will be expected to provide passwords to allow access to their devices if necessary.

- Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

1.15 Acceptable use of the internet in school

- All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 3, 4 and 5). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

- MSTeams is the virtual learning environment used at Bennett. It aims to improve the home-school link and make learning outside of lessons easier and more accessible. The school offers opportunities for teachers, parents and students to learn how to use MSTeams.

1.16 Students using mobile devices in school

- Students may bring mobile devices into school, but are not permitted to use them during the school day. This includes:

  - Lessons
  - Tutor group time
  - Clubs before or after school, or any other activities organised by the school
  - Break or lunchtime

- Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device. Parents may be required to collect any confiscated device.

1.17 Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the ICT manager. Work devices must be used solely for work activities.

1.18 How the school will respond to issues of misuse

- Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

- Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Appendix 1: Online Safety – Code of Conduct

This code of conduct applies at all times, whilst using school equipment. User areas on the network will be monitored and the school reserves the right to delete unsuitable files, intercept e-mails and to block sites considered inappropriate in school. All users are required to follow the conditions laid down in the policy. Any breach of the conditions may lead to withdrawal of the user's access to the network as well as the Internet and will also be considered a disciplinary matter.

General Network Use

- Only access the network using your own username and password, which must not be given to any other person.
- Do not trespass into other users' files or folders.
- Check work for accuracy before printing and avoid wasting paper by unnecessary printing.
- Treat the computers with respect – any attempt to damage equipment will result in disciplinary action.
- Only work data files may be loaded from a memory stick into your area.
- Do not use the network in any way that would disrupt use of the network by others.
- Use of a computer system without permission or for a purpose not agreed by the school could be a criminal offence under the Computer Misuse Act 1990.
- Inform a member of staff immediately if a security problem is identified. Do not demonstrate this problem to others.
- Students' Personal Computer equipment must not be plugged into the school network without prior consultation with the ICT Technical staff.

Internet Access

- Only sites that are appropriate for educational use should be accessed.
- The internet may only be used under supervision. 6th Form are allowed unsupervised access but the privilege will be withdrawn immediately should this be abused.
- Files must not be downloaded without permission from the teacher concerned.
- Copyright and trademarks must be respected. Text and pictures must not be copied from the Internet without acknowledging their source.
- No unauthorised software or games may be downloaded or played on the school computers.

E-Mail

- Users are responsible for e-mail they send and for contacts made. E-mail must be carefully written and polite.
- There must be no sending, accessing, creating or displaying of offensive language, sounds or images which are likely to cause offence, inconvenience or needless anxiety.
- E-mail may only be sent using the official school e-mail address:- username@bennett.kent.sch.uk Anonymous messages must not be sent. E-mail use is provided primarily for educational purposes.
- No home addresses, telephone numbers, personal information or photographs of yourself or others may be given to any strangers contacted over the network.
- Any unpleasant messages or material received must be reported immediately to a member of staff. Check with a teacher before opening any e-mail attachments or completing online questionnaires or subscription forms.

Disclaimer

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damage suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

Appendix 2: Acceptable use agreement (students)

Acceptable Use of the School’s ICT Systems and Internet: Agreement for Students	
When using the school’s ICT systems and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher’s permission • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school’s network using someone else’s details If I bring a personal mobile phone or other personal electronic device into school e.g. smart watch: • I understand that I must not use it during the school day and it should be switched off at all times • If I use my mobile phone or smart watch without permission it will be confiscated • If, despite the rules, I use my mobile phone or device to access the school network I understand that the websites I visit are visible to the school without the need to look at my device 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 cybercrime, such as hacking accounts or systems or sending abusive, threatening or offensive messages, or sharing inappropriate images can be a criminal offence. I will immediately let a teacher or other member of staff know if I find any material, which might upset, distress or harm me or others. I will always use the school’s ICT systems and internet responsibly.	
Student Name:	
Signed (student):	**Date:**

Top tips for keeping safe on-line

- Be careful about what you share on-line. Only chat to people you have actually met.
- Never give personal information (including name, address or telephone number) to anyone without the permission of your parent/carer
- Never arrange to meet anyone offline without first consulting with your parent/carer, or without adult supervision
- Always report anything that makes you feel uncomfortable

Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the School’s ICT Systems and the Internet:
Agreement for Staff, Governors, Volunteers and Visitors

Name of staff member/governor/volunteer/visitor:

When using the school’s ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school’s reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school’s network using someone else’s details

I will only use the school’s ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school’s ICT systems and internet responsibly, and ensure that students in my care do so too.

I have read and understood the staff code of conduct, which is published as part of the staff handbook

Signed (staff member/governor/volunteer/visitor):

Date: