

WHOLE SCHOOL ONLINE SAFETY POLICY

1 Scope

The School is committed to promoting and safeguarding the welfare of all students and an effective online safety strategy is paramount to this. This is particularly important with regard to the Prevent strategy, as a large portion of cases of radicalisation occur via online activities.

1.1 Aims

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

- to protect the whole School community from illegal, inappropriate and/or harmful online content or contact
- to educate the whole School community about online safety
- to establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

In considering the scope of the School's online safety strategy, the School will take a wide and purposeful approach to defining the technology, networks and devices used for viewing or exchanging information, including communications technology (collectively referred to in this policy as Technology).

This policy applies to members of the School community, including staff and volunteers, students, 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 students or any member of the School community or where the culture or reputation of the School is put at risk.

1.2 Relevant policies

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

- *Acceptable Use of Technology Policy for Students*
- *Safeguarding and Child Protection Policy and Procedures*
- *Anti-Bullying Policy including Anti-Cyberbullying*
- *Code of Conduct for Staff*
- *AI Guidelines*

2 Roles and responsibilities

2.1 The Governing Body

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

The Link Governor for Safeguarding has leadership responsibility for the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Governing Body.

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 above.

2.2 Principal and Senior Leadership and Management Team

- The Principal has overall executive responsibility for the safety and welfare of members of the School community.
- The Lead DSL is responsible for managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's *Safeguarding & Child Protection Policy and Procedures*.
- The Heads of Division/Director of Boarding/ DSLs/DDSLS will work, and meet with, the Head of Computer Science and the IT Manager in monitoring Technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and wellbeing of students.
- The Heads of Division/DSLs/DDSLS will regularly monitor any Technology incidents via MyConcern and use the school's filtering and monitoring system: Lightspeed.
- The Lead DSL will regularly update other members of the SLMT on the operation of the School's safeguarding arrangements, including online safety practices.

2.3 IT Manager

The IT Manager, together with their team, is responsible for the effective operation of the School's filtering system so that students and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

The IT Manager is responsible for ensuring that:

- the School's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack
- the user may only use the School's Technology if they are properly authenticated and authorised
- the School has an effective filtering and monitoring systems in place and that are applied and updated on a regular basis
- the risks of students and staff circumventing the safeguards put in place by the School are minimised
- 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
- filtering and monitoring software and systems are kept up to date to allow the team to monitor the use of email and the internet over the School's network and maintain logs of such usage

The IT Manager will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the School to safeguarding issues.

The IT Manager will report regularly to the Lead DSL on the operation of the School's Technology. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the School, they will escalate those concerns promptly to the appropriate members(s) of the School's Senior Leadership and Management Team (SLMT).

2.4 All staff

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

Staff have a responsibility to report any concerns about a student's welfare and safety in accordance with this policy and the School's *Safeguarding & Child Protection Policy and Procedures* to the Lead DSL.

2.5 Parents

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

- support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures
- 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
- 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

If parents have any concerns or require any information about online safety, they should contact the relevant Head of Division/Lead DSL.

3 Education and training

3.1 Students

The safe use of Technology is integral to the School's curriculum. Students 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 *Acceptable Use of Technology Policy for Students* and *PSHEE Policy*).

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

- about the risks associated with using Technology and how to protect themselves and their peers from potential risks
- how to protect their personal information and privacy online, including the safe use of passwords, privacy settings and multi-factor authentication
- how to recognise online scams, phishing, fraud and other attempts to obtain personal information
- how to communicate safely and respectfully online, including when using social media, messaging platforms and online gaming
- how to recognise misinformation, disinformation and content generated using artificial intelligence (AI), and to evaluate the reliability of online sources
- the importance of obtaining consent before sharing images, videos or personal information about themselves or others
- how to recognise inappropriate, harmful or illegal online content and the importance of reporting concerns promptly
- to be critically aware of content they access online and guided to validate accuracy of information
- how to recognise suspicious, bullying, radicalising and extremist behaviour
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect
- the consequences of negative online behaviour
- how to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly

The School's *Acceptable Use of ICT Policy for Students* sets out the School rules about the use Technology including internet, email, social media and mobile electronic devices, helping students to protect themselves and others when using Technology. Students are reminded of the importance of this policy on a regular basis.

3.2 Staff

- The School provides training on the safe use of Technology to staff so that they are aware of how to protect students and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.
- Staff receive training on the *Code of Conduct for Staff* and data protection guidance at induction and at regular intervals afterwards.
- 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.

3.3 Parents

- Information is available to parents via the Firefly portal. Additionally, we offer the opportunity for parents to attend School based sessions on online safety on a regular basis.
- Parents are encouraged to read the *Acceptable Use Policy for Students* with their child to ensure that it is fully understood.

3.4 Useful resources

There are useful resources about the safe use of Technology available via various documents and websites including:

- <http://www.thinkuknow.co.uk/>
- <https://www.disrespectnobody.co.uk/>
- <http://www.saferinternet.org.uk/>
- <https://www.internetmatters.org/>
- <http://educateagainsthate.com/>
- <http://www.childnet.com/resources>
- Keeping Children Safe in Education (DfE) – the statutory safeguarding guidance for schools.
- Teaching Online Safety in Schools (DfE) – non-statutory guidance on teaching online safety.
- Filtering and Monitoring Standards for Schools and Colleges (DfE)
- NSPCC Online Safety
- CEOP – Child Exploitation and Online Protection: reporting and educational resources from the National Crime Agency
- *DfE's Advice for head teachers and School staff on cyberbullying*
- *DfE's Advice for parents and carers on cyberbullying*
- *DfE's Advice on the use of social media for online radicalisation*
- *DfE's Guidance on mobile phones in schools*

4 Access to the School's Technology

The School provides internet and intranet access and an email system to students and staff as well as other Technology. Students and staff must comply with the respective *Acceptable Use of Technology Policy for Students* and the *Code of Conduct for Staff* when using School Technology. All such use is monitored by the IT Manager and their team.

Students and staff require individual user names and passwords to access the School's internet and intranet sites and email system which must not be disclosed to any other person. Any student or member of staff who has a problem with their user names or passwords must report it to the IT Department immediately.

No laptop, tablet or other mobile electronic device may be connected to the School network without the consent of the IT Manager. All devices connected to the School's network should have current and up-to-date anti-virus software installed and have the latest OS updates applied. The use of any device connected to the School's network will be logged and monitored by the IT Department.

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 by the IT Department.

4.1 Use of mobile electronic devices

The School has appropriate filtering and monitoring systems in place to protect students using the internet (including email text messaging and social media sites) when connected to the School's network. Mobile devices equipped with a mobile data subscription can, however, provide students with unlimited and unrestricted access to the internet. Students are not permitted to use their mobile phones during the School day.

The School rules about the use of mobile electronic devices are set out in the *Acceptable Use of Technology Policy for Students*.

The use of mobile electronic devices by staff is covered in the *Code of Conduct for Staff*. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.

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

5 Procedures for dealing with incidents of misuse

Staff, students 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.

5.1 Misuse by students

Anyone who has any concern about the misuse of Technology by students should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the *Anti-Bullying Policy including Cyberbullying* where there is an allegation of cyberbullying.

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

5.2 Misuse by staff

Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's *Whistleblowing Policy* or *Low-Level Concerns Policy* so that it can be dealt with in accordance with the staff disciplinary procedures.

If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the *Allegations of Abuse Against Teachers & Other Staff Policy*.

5.3 Misuse by any user

Anyone who has a concern about the misuse of Technology by any other user should report it immediately.

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.

If the School considers that any person is vulnerable to radicalisation, the School will make a referral 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.

6 Monitoring and review

Serious incidents involving the use of Technology will be logged centrally on MyConcern.

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

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