St Peter’s School
YORK

Online Safety Policy

St Peter's School, York

March 2024

(Next review Summer Term 2025)

1 Scope

1.1 St Peter's School, York comprises St Peter’s 2-8 (for pupils aged 2 to 8 years), St Peter's 8-13 (for pupils aged 8 to 13 years) and St Peter's 13-18 (for pupils aged 13 to 18 years), collectively referred to in this policy as **the School** unless otherwise stated.

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

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

1.3.1 To protect the whole School community from potentially illegal, inappropriate and harmful content or contact;

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

1.3.3 To establish effective mechanisms to identify, intervene and escalate concerns where appropriate; and

1.3.4 To help promote a whole school culture of openness, safety, equality and protection.

1.4 This policy forms part of the School’s whole school approach to promoting child safeguarding and wellbeing, which involves everyone at the School and seeks to ensure that the best interests of pupils underpins and is at the forefront of all decisions, systems, processes and policies.

1.5 Online safety is a running and interrelated theme throughout the devising and implementation of many of the School's policies and procedures (including its Child Protection and Safeguarding Policy and Procedures) and careful consideration has been given to ensure that it is also reflected in the School's curriculum, teacher training and any parental engagement, as well as the role and responsibility of the School's Designated Safeguarding Lead (and any deputies).

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

1.7 Reference to **staff** includes all those who work for or on behalf of the School, regardless of their employment status, including contractors, supply staff, volunteers and Governors unless otherwise indicated.

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

1.9 Although this policy is necessarily detailed, it is important that our safeguarding related policies and procedures are transparent, clear and easy to understand for staff, pupils, parents and carers. The School welcomes feedback on how we can continue to improve our policies.

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

1.10.1 Acceptable Use Policy for Pupils

1.10.2 Staff IT Acceptable Use Policy and Social Media Policy

1.10.3 Child Protection and Safeguarding Policy and Procedures

1.10.4 Anti-bullying Policy

1.10.5 Risk Assessment Policy for Pupil Welfare

1.10.6 Staff Code of Conduct

1.10.7 Data Protection Policy for Staff

1.10.8 School Rules and Guidelines

1.10.9 Behaviour and Discipline Policy

1.10.10 Relationships and Sex Education Policy

1.10.11 Use of mobile phones and cameras in the EYFS setting - EYFS only as referenced in the Child Protection and Safeguarding Policy 20.1.

2 Regulatory framework

2.1 This policy has been prepared to meet the School's responsibilities under:

2.1.1 Education (Independent School Standards) Regulations 2014

2.1.2 National minimum standards for boarding schools (Department for Education (DfE), September 2022)

2.1.3 EYFS Statutory framework for group and school based providers (DfE, January 2024)

2.1.4 Education and Skills Act 2008

2.1.5 Children Act 1989

2.1.6 Childcare Act 2006

2.1.7 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)

2.1.8 Equality Act 2010.

2.2 This policy has regard to the following guidance and advice:

2.2.1 Keeping children safe in education (DfE, September 2023) (KCSIE)

2.2.2 Preventing and tackling bullying (DfE, July 2017)

2.2.3 Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Digital, Culture, Media & Sport (DfDCMS) and UK Council for Internet Safety (UKCIS), December 2020)

2.2.4 Prevent duty guidance: for England and Wales (Home Office, October 2023, in force on 31 December 2023);

2.2.5 Channel duty guidance: protecting people susceptible to radicalisation (Home Office, October 2023)

2.2.6 Searching, screening and confiscation: advice for headteachers, school staff and governing bodies (DfE, July 2022, in force from September 2022)

2.2.7 Behaviour in schools: advice for headteachers and school staff 2022 (DfE, October 2022)

2.2.8 Safeguarding children and protecting professionals in early years settings: online safety considerations (UK CIS, February 2019)

2.2.9 Relationships Education, Relationships and Sex Education (RSE) and Health Education Guidance (DfE, Sept 2021)

2.2.10 Meeting digital and technology standards in education (DfE, March 2023)

2.2.11 Teaching online safety in schools (DfE, January 2023)

2.2.12 Harmful online challenges and online hoaxes (DfE, February 2021)

2.2.13 Online safety guidance if you own or manage an online platform (DfDCMS, June 2021)

2.2.14 A business guide for protecting children on your online platform (DfDCMS, June 2021)

2.2.15 Using External Expertise to Enhance Online Safety Education (UKCIS, October 2022)

2.2.16 Online safety in schools and colleges: questions from the governing board (UKCIS, October 2022)

2.2.17 Online safety audit tool (UKCIS, October 2022)

2.2.18 Appropriate filtering for education settings (UKCIS, May 2023)

2.2.19 Appropriate monitoring for schools (UKSIC, May 2023)

2.2.20 Online Safety Self-Review Tool for Schools, 360safe.

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

3 Roles and responsibilities

3.1 The Governing Body

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

Governing Body has overall responsibility for all matters which are the subject of this policy and for approving and reviewing its effectiveness.

3.1.2 The Senior Leadership Team, Designated Safeguarding Lead and IT service providers and responsible governors are responsible for reviewing the filtering and monitoring provision at the School as required, and at least annually.

3.1.3 The Designated Safeguarding Lead is responsible for monitoring the implementation of the policy (including the records of incidents involving the use of technology and logs of internet activity and sites visits, relevant risk assessments and any action taken in response and evaluating effectiveness, as required and at least termly.

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

3.1.5 The Nominated Safeguarding Governor is the senior board level lead with leadership responsibility for the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Governing Body.

3.1.6 The Governing Body will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in paragraph 1.3 above.

3.2 Head Master and Senior Leadership Team

3.2.1 The Head Master has overall executive responsibility for the safety and welfare of members of the School community. This includes a specific responsibility to ensure that the school has an effective filtering policy in place that is applied and updated on a regular basis.

3.2.2 The Designated Safeguarding Lead is a senior member of staff with lead responsibility for safeguarding and child protection, including online safety and understanding filtering and monitoring systems in place in school.

3.2.3 The responsibility of the Designated Safeguarding Lead includes:

(a) managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Child Protection and Safeguarding Policy and Procedures.

(b) ensuring all staff are appropriately trained and aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.

(c) working with the IT Operations Manager (see below) in monitoring Technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

(d) overseeing and acting on: filtering and monitoring reports, safeguarding concerns and checks to filtering and monitoring systems.

(e) regularly monitoring the Technology Incident Log maintained by the IT Operations Manager.

(f) regularly updating other members of the School's Senior Leadership Team and the Governing Body on the operation of the School's safeguarding arrangements, including online safety practices.

(g) providing training and advice for governors / staff / parents / carers / learners.

(h) promoting an awareness of and commitment to online safety education / awareness raising across the School and beyond.

3.3 IT Operations Manager

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

3.3.2 The IT Operations Manager is responsible for ensuring that:

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

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

(c) maintaining filtering and monitoring systems, providing filtering and monitoring reports and completing actions following concerns or checks to systems;

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

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

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

3.3.3 The School's firewall and web filter policies are applied to all users of the School's network and internet access route. There are different policies depending on the group to which the user account belongs to, staff or pupil. Pupil requests for over-rides to the filtering policy must come via a member of staff and be for educational purposes. Staff can, by written request, obtain an over-ride or re-assignment of filtering category for their own or their pupils' curricular needs. IT staff may test the requested resource for appropriate type of content in line with an educational resource and escalate if they feel it is not in line with 'normal' educational needs.

3.3.4 The pupil policy does not allow access to uncategorised web sites. Sites are initially categorised by the web filter provider and regularly updated to keep the 'whitelist' and black lists current. Most types of sexual, violent, intolerant, suspicious, malicious or illegal content is banned for all users. A limited amount of sex education and drugs in nutrition are allowed for educational purposes.

3.3.5 The IT Operations Manager will report regularly to the Senior Leadership Team on the operation of the School's Technology. If the IT Operations Manager has concerns about the functionality, effectiveness, appropriateness or use of Technology within the School, including the monitoring and filtering systems in place, he will escalate those concerns promptly to the Designated Safeguarding Lead.

3.3.6 The IT Operations manager is responsible for maintaining the Technology Incident Log (a central record of all serious incidents involving the use of technology) and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's Child Protection and Safeguarding Policy and Procedures.

3.4 All staff

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

3.4.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in paragraph 1.10 above.

3.4.3 Training for staff includes online safety which, amongst other things, includes an understanding of filtering and monitoring provisions in place, how to manage them effectively, how to escalate concerns when identified and any particular expectations or responsibilities in relation to filtering and monitoring.

3.4.4 All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

3.4.5 Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school. Examples of such abuse can include:

(a) the sending of abusive, harassing and misogynistic messages;

(b) the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery;

(c) the sharing of abusive images and pornography to those who do not wish to receive such content;

(d) cyberbullying.

3.4.6 Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:

(a) facilitates, threatens and / or encourages physical abuse;

(b) facilitates, threatens and / or encourages sexual violence; or

(c) is used as part of initiation / hazing type violence and rituals.

3.4.7 It is important that staff recognise the indicators and signs of child-on-child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child-on-child abuse at the School, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.

3.4.8 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*" or "*boys being boys*" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse.

3.4.9 The School has a **zero tolerance approach** towards child-on-child abuse (including in relation to sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's Behaviour and Discipline Policy and also as a safeguarding matter under the School's Child Protection and Safeguarding Policy and Procedures.

3.4.10 Staff have a responsibility to report any concerns about a pupil's welfare and safety to the Designated Safeguarding Lead and in accordance with this policy and the School's Child Protection and Safeguarding Policy and Procedures. If staff have any concerns regarding child-on-child abuse or if they are unsure as to how to proceed in relation to a particular incident, they should always speak to the Designated Safeguarding Lead in all cases.

3.5 Parents

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

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

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

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

3.5.2 If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Lead.

4 Filtering and Monitoring

4.1 Whilst considering their responsibility to safeguard and promote the welfare of pupils and provide them with a safe environment in which to learn, the Governing Body will do all it reasonably can to limit pupil's exposure to risks from the School's IT system. As part of this process the School has appropriate filtering and monitoring systems in place and regularly reviews their effectiveness.

4.2 The School has regard to Government filtering and monitoring standards, which require that the School:

4.2.1 identifies and assigns roles and responsibilities to manage filtering and monitoring systems;

4.2.2 reviews filtering and monitoring provision at least annually;

4.2.3 blocks harmful and inappropriate content without unreasonably impacting teaching and learning; and

4.2.4 has effective monitoring strategies in place that meet their safeguarding needs.

4.3 The School manages access to content across its systems for all users, including guest accounts. Logs / alerts are regularly reviewed and acted upon.

4.4 The School has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.) Younger learners use child friendly/age-appropriate search engines e.g. SWGfL Swiggle.

4.5 Access to content through non-browser services e.g. apps and other mobile technologies is managed in ways that are consistent with this policy.

4.6 The School has monitoring systems in place to protect the School, systems and users. It monitors all network use across all its devices and services. Logs/alerts are regularly reviewed and acted upon.

4.7 The School uses a number of monitoring strategies to minimise safeguarding risks on internet connected devices, including:

4.7.1 physical monitoring by staff watching screens of users;

4.7.2 live supervision by staff on a console with device management software;

4.7.3 network monitoring using log files of internet traffic and web access; and

4.7.4 individual device monitoring through software or third-party services.

5 Education

5.1 The teaching of online safety is integrated, aligned and considered as part of the whole-school safeguarding approach and wider staff training and curriculum planning.

5.2 The School ensures that children are taught how to keep themselves and others safe, including online, and the safe use of Technology is therefore integral to the School's ICT and PSHE curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices (see the School's Curriculum Policy). Teaching is tailored to the specific needs and vulnerabilities of individual children, such as those who are victims of abuse, children with SEN or disabilities.

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

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

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

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

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

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

5.4.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "*banter*" or "*just boys being boys*";

5.4.3 to be critically aware of content they access online and guided to validate accuracy of information;

5.4.4 how to recognise suspicious, bullying or extremist behaviour;

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

5.4.6 the consequences of negative online behaviour;

5.4.7 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly; and

5.4.8 how to respond to harmful online challenges and hoaxes.

5.5 The School recognises the crucial role it plays in relation to preventative education and that this is most effective in the context of a whole-school approach that prepares pupils for a life in modern Britain and creates a culture of zero tolerance for sexism, misogyny/misandry, homophobia, biphobia and sexual violence and sexual harassment.

5.6 Pupils are taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element. The School has a zero tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's Behaviour and Discipline Policy and also as a safeguarding matter under the School's Child Protection and Safeguarding Policy and Procedures.

5.7 Those parts of the curriculum which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

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

5.9 The School recognises that effective education needs to be tailored to the specific needs and vulnerabilities of individual pupils, including those who are victims of abuse, and those with special educational needs and disabilities, and this is taken into account when devising and implementing processes and procedures to ensure the online safety of its pupils. For more details on the School's approach, see School's Child Protection and Safeguarding Policy and Procedures and RSE and PSHE policies.

5.10 **Useful online safety resources for pupils**

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

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

5.10.3 https://childnet.com/resources/smartie-the-penguin

5.10.4 https://www.childnet.com/resources/digiduck-stories

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

5.10.6 https://mysafetynet.org.uk

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

5.10.8 https://www.bbc.com/ownit

6 Training

6.1 Governing Body

6.1.1 To ensure that all Governors are equipped with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures of the School are effective and that they support the delivery of a robust whole school approach to safeguarding, all Governors receive appropriate safeguarding and child protection (including online safety) training at induction. This training is regularly updated.

6.2 Staff

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

6.2.2 Induction training for new staff includes training on the School's online safety strategy including this policy, the Staff Code of Conduct, Staff IT Acceptable Use Policy and Social Media Policy. Training specifically addresses the School's filtering and monitoring provisions in place, how to manage them effectively, how to escalate concerns when identified and any particular staff expectations or responsibilities.

6.2.3 Staff training is regularly updated and ongoing staff development training includes (but is not limited to) training on Technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and/or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes. This training may be in addition to the regular safeguarding and child protection (including online safety) updated as required at induction and at least annually thereafter.

6.2.4 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and wellbeing issues, including those involving the use of technology., and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

6.2.5 Where safeguarding incidents involve an online element, such as youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the School's policy on sharing nudes and semi-nude images and videos as set out in the Child Protection and Safeguarding Policy and Procedures and *Searching, screening and confiscation: advice for schools*. In certain cases, it may be appropriate for staff to confiscate a pupil's devices to preserve any evidence and hand it to the police for inspection.

6.2.6 Staff are encouraged to adopt and maintain an attitude of 'it could happen here' where safeguarding is concerned, including in relation to sexual violence and sexual harassment and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and / or violent behaviour in the future.

6.2.7 Staff are trained to look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, the School will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within the School that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and / or staff training will be delivered to minimise the risk of it happening again.

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

6.2.9 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.

6.3 Parents

6.3.1 The School is in regular contact with parents and carers and uses its communications to reinforce the importance of ensuring that children are safe online. The School aims to help parents understand what systems are in place to filter and monitor their child's online use and ensures that parents are aware of what their children are being asked to do online (including what sites they will be asked to access) and who from the School they will be interacting with online, if anyone.

6.3.2 The School organises a number of evening presentations for parents by experts on social media and online safety, as well as sending out by email appropriate information from organisations such as CEOP and the UK Safety Internet Centre.

6.3.3 Parents are encouraged to read the Policy for Pupils on the Safe and Acceptable Use of ICT with their son / daughter to ensure that it is fully understood.

6.4 Useful resources for staff and parents

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

(a) http://www.thinkuknow.co.uk/

(b) https://www.disrespectnobody.co.uk/

(c) http://www.saferinternet.org.uk/

(d) https://www.internetmatters.org/

(e) https://www.commonsensemedia.org/

(f) http://www.askaboutgames.com

(g) http://educateagainsthate.com/

(h) http://www.kidsmart.org.uk/

(i) http://www.safetynetkids.org.uk/

(j) http://www.safekids.com/

(k) https://www.ceop.police.uk/safety-centre

(l) Advice for parents and carers on cyberbullying (DfE, November 2014)

(m) Cyberbullying: advice for head teachers and school staff (DfE, November 2014)

(n) Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)

(o) Online safety in schools and colleges: questions from the governing board (UKCIS, October 2022)

(p) Education for a connected world framework (UKCIS, June 2020)

(q) https://www.lgfl.net/online-safety/resource-centre

(r) Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)

(s) Myth vs Reality: PSHE toolkit (Childnet, April 2019)

(t) SELMA Hack online hate toolkit (SWGFL, May 2019)

(u) Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects (DfE, January 2023)

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

(w) Harmful online challenges and online hoaxes (DfE, February 2021)

(x) Professionals online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772.

(y) NSPCC helpline for anyone worried about a child - 0808 800 5000

(z) Internet Watch Foundation - internet hotline for the public and IT professionals to report potentially criminal online content

(aa) LGfL: parents - scare or prepare

(bb) Thinkuknow: what to do if there's a viral scare online

6.4.2 The City of York Safeguarding Children Partnership has produced guidance for parents on radicalisation which is available here: http://www.saferchildrenyork.org.uk/advice---supporting-and-safeguarding-children.htm.

7 Access to the School's Technology

7.1 The School provides internet and intranet access and an email system to pupils and staff as well as other Technology. Pupils and staff must comply with the respective Acceptable Use Policy when using School Technology. All such use is monitored by the ICT team.

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

7.3 No laptop or other mobile electronic device may be physically connected to the School network without the consent of the ICT team. Senior school pupils and all boarders are able to connect personal devices to the Wi-Fi network by use of their school User ID and password. Pupils' devices are expected to have an up to date, in support, operating system. If no anti-virus product is apparent they are advised to download and install a free one as soon as possible. The use of any device connected to the School's network will be logged and monitored by the ICT team.

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

7.5 **Inappropriate material**

7.5.1 The School recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

7.5.2 Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the Designated Safeguarding Lead. The term 'online safety' encapsulates a wide range of ever evolving issues but these can be classified into four main areas of risk:

(a) **Content** - being exposed to illegal, inappropriate or harmful content (e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism);

(b) **Contact** - being subjected to harmful online interaction with other users (e.g. peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom and / or exploit them for sexual, criminal, financial or other purposes);

(c) **Conduct** - online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as the consensual and non-consensual sharing of nudes and semi-nudes and / or pornography), sharing other explicit images and online bullying; and

(d) **Commerce** - risks such as online gambling, inappropriate advertising, phishing and / or financial scams.

7.6 **Use of mobile electronic devices**

7.6.1 The School has appropriate filtering and monitoring systems in place to protect pupils using the Internet when connected to the School's network. Mobile devices equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet.

7.6.2 Whilst the use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while on the School premises is allowed, we encourage pupils to use the School's wi-fi network so that they benefit from the School's filtering and anti-virus software. Pupils accessing the internet outside the School's network whilst on School premises or otherwise in the care of the School do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour.

7.6.3 The School rules about the use of mobile electronic devices are set out in the Policy for Pupils on the Safe and Acceptable Use of ICT.

7.6.4 The use of mobile electronic devices by staff is covered in the Code of Conduct, IT Acceptable Use Policy, Social Media Policy, and Data Protection Policy 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 or when registering pupils through the SOCS or iSAMS apps.

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

8 Procedures for dealing with incidents of misuse

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

8.2 The School recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously. Staff should however be careful not to promise that a concern will be dealt with confidentially at an early stage as information may need to shared further (e.g. with the Designated Safeguarding Lead) to discuss next steps.

8.3 Misuse by pupils

8.3.1 Anyone who has any concern about the misuse of Technology by pupils should report it to the appropriate member of staff (referred to in the table below) so that it can be dealt with in accordance with the School's Behaviour and Discipline policies, including the Anti-bullying Policy where there is an allegation of cyberbullying:

Type of misuse	Relevant policy	Reporting channel
Bullying	Anti-Bullying Policy	Housemaster / Housemistress, Form Teacher/ Mentor Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead
Sharing nudes and semi-nude images (sexting/youth produced sexual imagery)	Child Protection and Safeguarding Policy and Procedures	Housemaster / Housemistress, Form Teacher/ Mentor Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters

Harassment	Child Protection and Safeguarding Policy and Procedures	Housemaster / Housemistress, Form Teacher/ Mentor Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Upskirting	Child Protection and Safeguarding Policy and Procedures	Housemaster / Housemistress, Form Teacher/ Mentor Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Radicalisation	Child Protection and Safeguarding Policy and Procedures	Housemaster / Housemistress, Form Teacher/ Mentor Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Other breach of acceptable use policy	See relevant policy referred to in Acceptable Use Policy for Pupils	Housemaster / Housemistress, Form Teacher/ Mentor Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters

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

8.4 Misuse by staff

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

8.4.2 Anyone who has any concern about the misuse of Technology by staff should report their concerns as set out below:

8.4.3 Staff should speak to their Line Manager in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures; and

(a) Anyone else should speak to the Head Master.

8.5 **Misuse by any user**

8.5.1 Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the Director of IT Operations or the Deputy Head.

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

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

9 Cybercrime

9.1 Cybercrime is criminal activity committed using computers and / or the internet. It is broadly categorised as either ‘cyber-enabled’ (crimes that can happen off-line but are enabled at scale and at speed on-line) or ‘cyber dependent’ (crimes that can be committed only by using a computer).

9.2 Cyber-dependent crimes include:

9.2.1 unauthorised access to computers (illegal ‘hacking’), for example, accessing a school’s computer network to look for test paper answers or change grades awarded;

9.2.2 denial of service (Dos or DDoS) attacks or ‘booting’, which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and

9.2.3 making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

9.3 The School is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

9.4 If staff have any concerns about a child in this area, they should refer the matter to the Designated Safeguarding Lead immediately. The Designated Safeguarding Lead should then consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not currently cover ‘cyber-enabled’ crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

10 Risk assessment

10.1 The School recognises that technology, and the risks and harms associated with it, evolve and change rapidly. The School will carry out regular, and at least annual, reviews of its approach to online safety, supported by risk assessments which consider and reflect the risks faced by their pupils.

10.2 Furthermore, where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

10.3 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

10.4 The Head Master has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

10.5 Day to day responsibility to carry out risk assessments under this policy will be delegated to the IT Operations Manager who have / has been properly trained in, and tasked with, carrying out the particular assessment.

11 Monitoring and review

11.1 All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

11.2 All serious incidents involving the use of Technology will be logged centrally in the Technology Incident Log by the Designated Safeguarding Lead and the Director of IT Operations.

11.3 The Designated Safeguarding Lead will consider the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the School are adequate.

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

11.5 The information created in connection with this policy may contain personal data. The School's use of this personal data will be in accordance with data protection law. The School has published privacy notices on its website which explain how the School will use personal data.

Authorised by	The Board of Governors March 2024
Next Review	Summer Term 2025