Online Safety Policy

LSA High School is committed to safeguarding and promoting the welfare of young people and expects all staff and volunteers to share this commitment.

Date Policy Agreed by Governing Body	January 2026
Date of Next Review	January 2028
Headteacher	Ben Corbett
Designated Safeguarding Lead/Online Safety Lead	Nigel Cross
Chair of Governors	Beverley Harrison

Contents:

Statement of intent

Lytham St Annes High School understands that using online services is an important aspect of raising educational standards, promoting student achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of students and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect students and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE 'Filtering and monitoring standards for schools and colleges'
- DfE 'Harmful online challenges and online hoaxes'
- DfE 'Keeping children safe in education 2025'
- DfE 'Teaching online safety in school'
- DfE 'Searching, screening and confiscation'
- DfE 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreements
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Mobile Phone Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy

2. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguarding Lead's (DSL) remit covers online safety.
- Reviewing this policy on a bi-annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and annually.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the Deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping students safe.
- Working with the DSL and ICT technicians to conduct light-touch reviews of this policy through the school's Safeguarding Committee.
- Working with the DSL and governing board to update this policy on a bi-annual basis.
- Identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems.
- Appointing an SLT digital lead in line with the Cyber-security Policy.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a yearly basis.
- Working with the headteacher and ICT technicians to conduct light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on a bi-annual basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct light-touch reviews of this policy.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours and adhering to the Staff Acceptable Use Agreement.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Students will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about students' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted at least yearly on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by students to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that students displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a student's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding and Child Protection Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising students, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a student has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain students can be more at risk of abuse and/or bullying online, such as lesbian, gay, bisexual, or gender questioning students and students with SEND.

Cyberbullying against students or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

5. Child-on-child sexual abuse and harassment

Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that students are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts

- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to students becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other students taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Safeguarding and Child Protection Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that students who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the student may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact students are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a student may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place

in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about students with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding and Child Protection Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain students at increased vulnerability to radicalisation and will act in line with the school's legal obligation under its Prevent duty.. Staff will be expected to exercise vigilance towards any students displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a student relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the safeguarding and Child Protection Policy and the school's Prevent duty.

7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a student's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a student is suffering from challenges in their mental health.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an "**online hoax**" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "**harmful online challenges**" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the student and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing students.
- Not inadvertently encouraging students to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger students but is almost exclusively being shared amongst older students.
- Proportional to the actual or perceived risk.
- Helpful to the students who are, or are perceived to be, at risk.
- Appropriate for the relevant students' age and developmental stage.
- Supportive.
- In line with the Safeguarding and Child Protection Policy.

Where the DSL's assessment finds an online challenge to be putting students at risk of harm, they will ensure that the challenge is directly addressed to the relevant students, e.g. those within a particular age range that is directly affected or individual students at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that students with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and

responsibilities relating to filtering and monitoring systems. All staff will be made aware that students are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among students.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support students in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

RSHE - Personal Development - ICT (Computing)

Online safety teaching is always appropriate to students' ages and developmental stages.

Students are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours students learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks students may face online are always considered when developing the curriculum.

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring students develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks

Students will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip students with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks

The school will educate students about the potential dangers of interacting with others online. Students will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose

as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks

Students will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Students will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks

The curriculum will also include education on online commercial risks. Students will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will be involved with the development of the school's online safety curriculum. Students will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for Looked After Children (LAC), will work together to ensure the curriculum is tailored so that students who may be more vulnerable to online harms, e.g. students with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from students.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting lessons or activities on online safety, the Head of Department and DSL will consider the topic that is being covered and the potential that students in the year (classes) have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the Head of Department how to best support any student who may be especially impacted by a lesson or activity. The Head of Department will then inform the class teacher and advise how best to deliver the lesson and support the student(s). Lessons and activities will be planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which students feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything students raise during online safety lessons and activities, they will make a report in line with the Safeguarding and Child Protection Policy.

If a student makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Safeguarding and Child Protection Policy.

12. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops /Tablets
- Email

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Students will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Students will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Acceptable Use Agreement for Students.

Staff will use all smart technology and personal technology in line with the school's Mobile Phone and Electronic Devices Policy.

The school recognises that students' unlimited and unrestricted access to the internet via mobile phone networks means that some students may use the internet in a way which breaches the school's acceptable use of ICT agreement for students.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Students will not be permitted to use smart devices or any other personal technology whilst in School.

Where it is deemed necessary, the school will ban student's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among students, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating students about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents/carers

The school will work in partnership with parents/carers to ensure students stay safe online at school and at home. Parents/carers will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be encouraged to go through the Acceptable Use Agreement for

Students with their child to ensure their child understands the document and the implications of not following it. Parents/carers will also be asked to agree to a parent/carer Acceptable Use Agreement.

Parents/carers will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of students, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents/carers will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Training sessions
- Newsletters
- Online resources

15. Internet access

Students, staff and other members of the school community must follow the terms of their Acceptable Use Agreement when accessing the School's network. Students will not be allowed access to the school network on their own personal devices.

16. Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the ICT Helpdesk. Prior to making any changes to the filtering system, ICT technicians will consider the implications of such changes and speak with and seek advice from the DSL and/or headteacher if necessary. Any changes made to the

system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a student has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Safeguarding and Child Protection Policy.

17. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls regularly to ensure they are running correctly, and to carry out any required updates.

Staff and students will be advised not to download software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Students will be provided with their own unique username and private passwords. Staff members and students will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users will inform ICT technicians if they forget their login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, they will be sanctioned in line with the Behaviour Policy.

Users will be required to lock access to devices and systems when they are not in use.

The SLT digital lead will be responsible for implementing appropriate network security measures in liaison with the DPO and DSL. Full details of the school's network security measures can be found in the Cyber-security Policy.

18. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff and students will be given approved school email accounts and will be authorised to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and students must agree to and sign the Acceptable Use Agreement. Personal email accounts must not be used by staff and students for school work/correspondence.

Staff members and students will be required to block spam and junk mail and report the matter to ICT technicians. Chain letters, spam and all other emails from unknown sources must be opened with caution and no links should be accessed and no information shared in response where the user has concerns. Where the user is unsure the advice of the ICT technicians should be sought and the email brought to their attention.

The school's Personal Development and Business and Computing programme will explain what a phishing email and other malicious emails might look like – it will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

19. Generative artificial intelligence (AI)

The school will take steps to prepare students for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to students' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit student's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that students are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into unapproved AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20. Social networking

The use of social media by staff and students will be managed in line with the school's Code of Conduct.

21. The school website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

22. Use of devices

Staff members and students will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Acceptable Use agreement and the loan of laptop protocols.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Student Mobile Phone and Electronic Devices Policy.

23. Remote learning

All remote learning will be delivered in line with this policy. This policy specifically sets out the school's approach to online safety and will be considered when delivering remote education.

24. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct regular light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL will review this policy in full on a bi-annual basis and following any online safety incidents.

The next scheduled review date for this policy is January 2028.

Any changes made to this policy are communicated to all members of the school community.