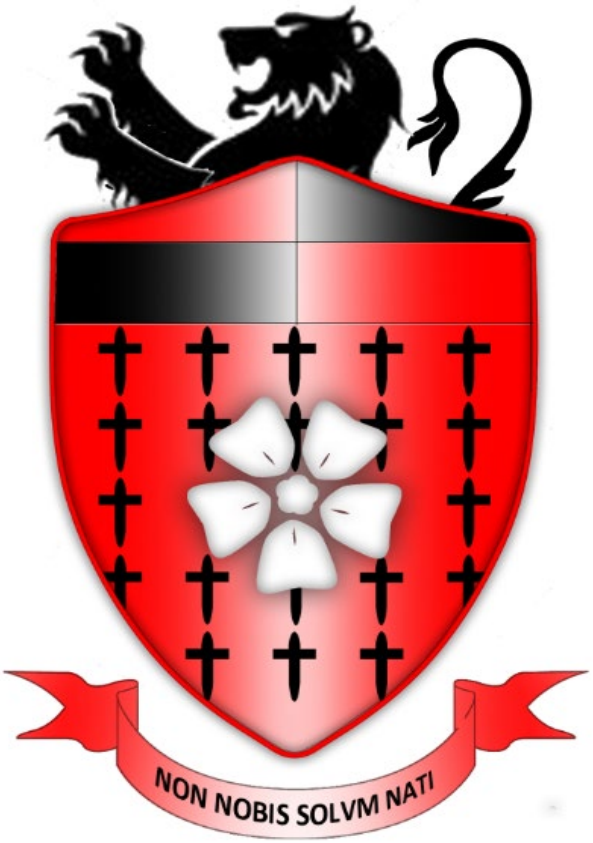
Hornsea School & Language College



E-Safety Policy

Last Reviewed:	Date: October 2025	By: Kay Sullivan
Approved by:	Headteacher: 26.11.25	Governing Body: 26.11.25
Date of Next Review:	November 2026	

Contents

1.Context

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access

Students will use the Internet outside school and will need to learn how to evaluate Internet information and be able to recognise and respond to risk in respect of their own safety and security.

As per KCSiE 2025, 'It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students and staff in their use of technology and establishes mechanisms to identify, intervene in and escalate any concerns where appropriate'.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient (online teaching and learning resources, facilitating 24:7 'anywhere' access)
- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between students world-wide
- Access to experts in many fields for students and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;

- Exchange of curriculum and administration data with the Local Authority and DCSF

How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for student use and includes filtering and monitoring appropriate to the age of students
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line activities that will support learning outcomes planned for the students' age and maturity
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

2. Aims

HSLC aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

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

3. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education September 2025, and its advice for schools.

The DSL has overall responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place; they

can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated.

• DSLs should evidence that they have accessed appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.
• All staff (including governors and trustees) should receive appropriate safeguarding and child protection training, including online safety at induction. This should amongst other things, include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
• Online safety should also be addressed as part of regular (at least annual) child protection training and staff should receive updates, as appropriate.
• Children should be taught about online safety, including as part of statutory Relationships and Sex Education (RSE), however schools and colleges should recognise that a one size fits all approach may not be appropriate, and a more personalised or contextualised approach for more vulnerable children e.g., victims of abuse and SEND, may be needed.
• Schools/colleges should be doing all that they reasonably can to limit children's exposure to risks from the school's or college's IT system and should ensure they have appropriate filtering and monitoring systems in place and regularly review their effectiveness. The leadership team and relevant staff should have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns identified. When making filtering and monitoring decisions, schools/colleges should consider those who are 'potentially at greater risk of harm' and how often they access the IT system along with the proportionality of costs versus safeguarding risks.
• Schools/colleges should recognise that child-on-child abuse, including sexual violence and sexual harassment can occur online. School/colleges have an essential role to play in both preventing online child-on-child abuse and responding to any concerns when they occur, even if they take place offsite and should have appropriate systems in place to support and evidence this.
• Schools/colleges should ensure their child protection policy and wider safeguarding policies specifically address online safety, especially with regards to appropriate filtering and monitoring on school devices and school networks, child-on-child abuse, relationships on social media and the use of mobile and smart technology.
• Schools/colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the specific risks their children face.

4. Roles and responsibilities

4.1 The Governing Body

- The Governing Body has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.
- The Governing Body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- The Governing Body will receive regular updates through the Link Governor for ESafety at HSLC, Graham McDonald, who will attend regular ESafety Steering Group meetings to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL), Kay Sullivan.

- The Governing Body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Governing Body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The Governors will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include identifying and assigning roles and responsibilities to manage filtering and monitoring systems;

- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Governor who oversees online safety is Graham McDonald.

- All governors will ensure they have read and understand this policy and agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

4.2 The Head Teacher

The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head Teacher and Governing Body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT Manager and HSLC Helpdesk to make sure the appropriate systems and processes are in place
- Working with the Head Teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy

- Working proactively to identify emerging themes and concerns, developing effective and targeted responses in collaboration with the ICT Manager, Life Studies Co-ordinator and HSLC Helpdesk
- Ensuring that any online safety incidents are logged appropriately on CPOMS and dealt with in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Ensuring relevant training to all members of the school community in respect of online safety and Smoothwall Filtering and Monitoring Systems
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head Teacher and/or Governing Body (termly)
- Providing regular safeguarding and child protection updates, including online safety, to all staff in order to continue to provide them with relevant skills and knowledge to safeguard effectively (HSLC Online Safety Hub).
- Support the HSLC ESafety Steering Group ensuring all members of the group have a full and thorough understanding of ESafety

4.4 The Network Manager

The Network Manager is responsible for putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
Conducting a full security check and monitoring the school's ICT systems on a regular basis
Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Positive Discipline policy

4.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting the DSL, Kay Sullivan either via CPOMS or sullivank@hslc.co.uk.
- Following the correct procedures by pro-actively contacting the DSL, Kay Sullivan, or the Network Manager, Rob Coles at Helpdesk@hslc.o.uk if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Positive Discipline Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Ensuring vigilance at all times when supporting pupils using devices or technology

4.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Contact the DSL, Kay Sullivan, should parents/carers have concerns about their child's use of the internet to ensure advice and guidance, supporting identified worries

4.7 Visitors and members of the community

Visitors and members of the community who use HSLC's ICT systems or internet will to follow the guidance within this policy. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Filtering and Monitoring

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system (KCSiE 2025)

Hornsea School and Language College will be using a professional, versatile proxy server that filters Web content using a number of techniques. These include real-time context analysis in multiple languages, a known database of categorised sites and sophisticated image content analysis.

Hornsea School uses SSL Intercept Mode. This is a means every time you visit a site in the form https://somesite.com the Smoothwall software will decrypt, check and re-encrypt the traffic before continuing communication with the target site. Sites excluded include banking etc.

As students progress through school they are given greater responsibility as the filtering of internet use is reduced. 6th Formers for example have access to YouTube to allow them to access its many educational resources They receive a letter to highlight the responsibility of this degree of filtering and are aware that this privilege could be removed if abused.

Impero network management software is used to monitor network users activities at all time. Key word libraries are used to safeguard users by capturing on screen activity and time stamping violations

6. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In KS3, pupils will be taught to:

Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in KS4 will be taught:

To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
How to report a range of concerns

By the end of secondary school, pupils will know:

Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
What to do and where to get support to report material or manage issues online
The impact of viewing harmful content
That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
How information and data is generated, collected, shared and used online
How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Internet Danger Awareness

All teaching staff and all pupils will be made aware of the potential dangers of online activity and trained using the National Online Safety Training. Annual online e-safety training is also completed by teaching staff.

A program of E-safety education will be delivered throughout the curriculum. It covers general e-safety, using ICT in the workplace in y10 and digital footprints in y11. These messages are supplemented and reinforced by assemblies on emerging safeguarding themes including 'sextortion'

Parents are also alerted to topical issues relating to internet danger by emails from the DSL. Online training is also offered to all parents through the shared NSPCC resource. All members of the HSLC community have access to the HSLC Online Safety Hub

Social Networking

- The School will block/filter access to social networking sites unless a specific use is approved by the head
- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students should be advised not to place personal photos on any social network space
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

7. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety through the HSLC Online Safety Hub or other communications home, and in information via our website information shared by third parties. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- The system the school uses to filter and monitor online use (Smoothwall)
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL, Kay Sullivan

Concerns or queries about this policy can be raised with any member of staff or the Head Teacher.

8. Cyber-bullying

8.1 Definition

Cyberbullying is bullying that takes place online. Unlike bullying offline, online bullying can follow the child wherever they go, via social networks, gaming and mobile phone. A person can be bullied online and offline at the same time. (NSPCC)

Cyberbullying can include (examples provided by NSPCC):

- sending threatening or abusive text messages
- creating and sharing embarrassing images or videos
- trolling – the sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding children from online games, activities or friendship groups
- shaming someone online
- setting up hate sites or groups about a particular child
- encouraging young people to self-harm
- voting for or against someone in an abusive poll

8.2 Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will

ensure that pupils know how they can report any incidents and are encouraged to do so through HSLC online platforms like The Big Red Button, including where they are a witness rather than the victim.

- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (Life Studies) education, and other subjects where appropriate.
- The school also sends information including advice on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Positive Discipline policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8.3 Examining electronic devices

The Head Teacher, and any member of staff authorised to do so by the Head Teacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL or Head Teacher
Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it in line with the HSLC Searching, Screening and Confiscation Policy.

Seek the pupil's co-operation whenever possible

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL, Head Teacher or member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves
- If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
    - Not view the image
    - Confiscate the device and report the incident to the DSL (or DDSL) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Any searching of pupils will be carried out in line with:
    - UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
    - HSLC Positive Discipline policy / HSLC Searching, Screening and Confiscation policy

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

8.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

HSLC recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

HSLC will treat any use of AI to bully pupils in line with our Positive Discipline Policy and Child on Child abuse policy. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.

9. Acceptable use of the internet in school

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- Staff must complete the Cyber security training & the Data Protection training.

- The school will maintain a current record of all staff and students who are granted Internet access
- Parents will be informed that students Internet access will be monitored and that it is not possible to filter all unsuitable sites
- Parents will be asked to update consent on Edulink for internet access.
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement
- All pupils have access to the guest Wi-Fi. Y11-13 have access to it during lesson time to allow them to use their own devices for research, for example during study periods. Y7-10 have access outside of lesson times. Filtering varies by year group and is age appropriate

Students who try to gain unauthorised access to the internet OR websites will be dealt with in line with the schools Positive Discipline Policy. However serious breaches may result in additional sanctions and referral to relevant organisations.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

HSLC will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

10. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

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

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Positive Discipline policy, which may result in the confiscation of their device.

11. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Not sharing the device among family or friends
- Staff members must not use the device in any way that would violate the school's terms of acceptable use
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from The Network Manager, Rob Coles, or HSLC Helpdesk

12. How the school will respond to issues of misuse

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

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

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

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required through the termly Safeguarding Newsletter

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
    - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

<u>Training will also help staff:</u>

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term
- The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.
- More information about safeguarding training is set out in our child protection and safeguarding policy.

14. Monitoring arrangements

The DSL and DDSL ensure accurate records for all behaviour and safeguarding issues related to online safety. This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Governing Body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies
This online safety policy is linked to our:

Child protection and safeguarding policy
Positive Discipline policy
Complaints procedure
ICT and acceptable use policy
Searching, Screening and Confiscation policy