

Online Safety Policy

THIS POLICY REFERS TO ALL STUDENTS INCLUDING THOSE IN EYFS

Contents

1. Aims	3
2. Legislation and guidance	4
3. Links with other policies	4
4. Roles and responsibilities	5
5. Educating students about online safety	7
6. Educating parents about online safety.....	9
7. Cyber-bullying, Child-on-child sexual violence & sexual harassment & upskirting	9
8. Acceptable use of the internet in school.....	11
9. Students using mobile devices in school	12
10. Staff using work devices outside school.....	12
11. How the school will respond to issues of misuse	13
12. Training	13
13. Filtering and Monitoring arrangements	14
14. Students' and Parents' Social Media Presence.....	15

1. Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Nottingham High School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping staff to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - for the protection and benefit of the children and young people in their care, and
 - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
 - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns, with reference to other school policies such as the Anti-Bullying Policy.

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors including through filtering and monitoring
- 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 managing 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

2. Legislation and guidance

This policy is based on the current Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for Headmasters and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

3. Links with other policies

This online safety policy is linked to our:-

- Safeguarding and Child Protection Policy (incl EYFS)
- Misbehaviour and Exclusions policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure for Parents Policy
- IT Acceptable Use policy (Students)
- IT Acceptable Use Policy (Staff)
- Off-Site Visits Policy
- Parent Contract
- Pastoral Care Policy
- Procedure on Taking, Storing and Using Images of Children
- Recruitment, Selection and Disclosures Policy
- Risk Assessment Policy
- Staff Code of Conduct Policy

- Anti-Bullying Policy (Senior).
- Curriculum Policy (Senior)
- Relationship Sex Education RSE Policy (Senior)
- Anti-Bullying Policy (IJS)
- Relationship Sex Education RSE Policy (Junior)
- Promoting Good Behaviour Policy (Junior)

4. Roles and responsibilities

4.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headmaster to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety information as provided by the Designated Safeguarding Lead (DSL).

The governor who oversees online safety is Gail Walton.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on the relevant IT acceptable use Policy
- 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 age appropriateness, vulnerable children, victims of abuse and some students 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 Headmaster

The Headmaster is responsible for ensuring that all affected persons understand this policy, and that it is being implemented consistently throughout the school.

4.3 The Designated Safeguarding Lead

Details of the School's Designated Safeguarding Lead (DSL) and deputies are set out in our Safeguarding and Child Protection Policy (incl EYFS) as well as relevant job descriptions.

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

- Supporting the Headmaster in ensuring that all affected persons understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headmaster, ICT manager and other staff and agencies, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with all relevant school policies.

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with relevant school policies.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headmaster and/or Governing Body.

This list is not intended to be exhaustive.

4.4 The ICT manager

The ICT manager, supported by IT staff, is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students 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 annually and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and content and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with relevant school policies.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school misbehaviour and exclusion policy.
- This list is not intended to be exhaustive.

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 IT Acceptable Use Policy (Staff), and ensuring that students follow the school's terms on IT acceptable use Policy (Students)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with relevant school policies.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school misbehaviour and exclusion 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'.

This list is not intended to be exhaustive.

4.6 Parents

Parents are expected to:

- Notify a member of staff or the Headmaster of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on all relevant policies and procedures as published on the school website.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

4.7 Visitors and members of the community

Visitors and members of the community who use the School's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Educating students about online safety

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

The text below is taken from the [National Curriculum computing programmes of study](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

In **Key Stage 1**, students will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Students in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of Junior school**, students will know:

- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, students will be taught to:

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

Students in **Key Stage 4** will be taught:

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

By the **end of secondary school**, students 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 which 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 which 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)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home. This policy will also be shared with parents via our website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Deputy Head (Individuals) in the Senior School and Deputy Head (Pastoral) in the Infant and Junior School.

Concerns or queries about this policy can be raised with the Deputy Head (Individuals) in the Senior School or Deputy Head (Pastoral) in the Infant and Junior School.

7. Cyber-bullying, Child-on-child sexual violence & sexual harassment & upskirting

7.1 Definition cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying is unwanted conduct of behaviour designed to cause harm or distress to another person. It can be characterised as offensive, intimidating, malicious or insulting behaviour, an abuse or misuse of power through means intended to undermine, humiliate, denigrate or injure the recipient. Bullying can be related to age, sex, race, disability, religion, sexual orientation, nationality or any personal characteristic of the individual, and maybe persistent or an isolated incident. The key is that the actions or comments are viewed as demeaning to the recipient. Further to Section 7.3 and Section 7.4, the list is not exhaustive and further information can be found in the Safeguarding and Child Protection Policy.

7.2 Preventing and addressing cyber-bullying

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

The School will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 12 for more detail).

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

The DSL will 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.

7.3 Child-on-child sexual violence and sexual harassment

Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment'. Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

In the online environment, the recent proliferation of content, such as misogynistic and misandrist content, is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

7.4 Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse, students can come and talk to members of staff if they have made a mistake or had a problem in this area.

7.5 Examining electronic devices

The Headmaster, and any member of staff authorised to do so by the Headmaster (as set out in your misbehaviour and exclusion policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students,
- Is identified in the school rules as a banned item for which a search can be carried out,
- 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 students and staff. If the search is not urgent, they will seek advice from the Headmaster and/or DSL.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's cooperation

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 staff member in conjunction with the DSL, Headmaster and/or other member of the Senior Management 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 student and/or the parent 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 equivalent) 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 students will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

8. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to agree to the acceptable use of the school's ICT systems and the internet. If appropriate, visitors will be expected to read and agree to the School's terms on acceptable use.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the IT acceptable use agreements.

9. Students using mobile devices in school

The School does all that it reasonably can to limit children's exposure to the risk identified above through the use of the School's network and has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email, and social media sites) when connected to the School's network.

However, mobile devices and smart technology equipped with a mobile data subscription (3G, 4G, 5G) can provide pupils with unlimited and unrestricted access to the internet. The School is alert to the risks that such access presents, including the risk of pupils sexually harassing, bullying or controlling their peers using their mobile or other smart technology; or sharing indecent images consensually or non-consensually (often via large group chats); or viewing and/or sharing pornography and other harmful content, and has mechanisms in place to manage such risks.

Senior Students may bring mobile devices into school, but are not permitted to use them during lessons/Form/Tutor Time unless instructed to by a teacher. Junior pupils may bring a mobile device into school if they require it for independent travel to and from school (such as on a school bus) or if permitted, on a school trips but are not permitted to use it at any point during the school day. Infant pupils are not permitted to bring mobile devices to school.

We recognise that students are allowed at our School to use their mobile devices more freely. Our philosophy is that education regarding the use of devices is valuable and an open culture will allow us to identify students who are addicted or using their devices inappropriately. Very few instances of bullying via online devices during school hours or in the school context are identified, for example. Staff are vigilant to the use of mobile devices around the school site and training reinforces the need for them to report any issues of concern. Any use of mobile devices in school by students must be in line with the IT Acceptable Use Policy and the BYOD Policy.

The School's policies apply to the use of technology 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. Any trends around misuse of personal devices not connected to the internet are considered for any educational opportunities to be taken and, should we identify trends relating to misuse of mobile devices, the School's policy around their use will be reviewed.

Any breach of the acceptable use agreement by a student may trigger disciplinary action which may result in the confiscation of their device.

10. 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:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing Antivirus updates.
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

If staff have any concerns over the security of their device, they must seek advice from the IT Manager.

11. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on misbehaviour and exclusion policy and IT Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff disciplinary procedures/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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. 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 (for example through emails, e-bulletins and staff meetings).

Updated guidance, such as KCSIE (2023) makes it clear that all staff should receive training on the expectations, applicable roles and responsibilities in relation to filtering and monitoring. The designated safeguarding lead will take lead responsibility for understanding the filtering and monitoring systems and processes in place. The guidance signposts the Department for Education's new filtering and monitoring standards (DfE, 2023b), which support the school to have effective systems in place. The school is working to meet the DfE's Cyber security standards for schools and colleges (DfE, 2023c).

By way of 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, 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

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse

- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies 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 Safeguarding and Child Protection Policy (incl EYFS).

13. Filtering and Monitoring arrangements

The School will provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding students and staff from potentially harmful and inappropriate online material. Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will work closely together with the School's IT service providers.

This policy will be reviewed at least annually by the Designated Safeguarding Lead or when a safeguarding risk is identified, there is a change in working practice or new technology is introduced. 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 students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

The School recognises that an effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not unreasonably impact teaching and learning or school administration or restrict our students from learning how to assess and manage risk themselves. The filtering system is operational, up to date and applied to all users, including guest accounts, school owned devices and devices using the school broadband connection. Our filtering systems allow us to identify the device name or ID, IP address, and where possible, the individual, the time and date of attempted access and the search term or content being blocked.

The DSL logs behaviour and safeguarding issues related to online safety. When inappropriate material or a concerning search term is used, staff are instantly notified in order to take appropriate action. The DSL will meet with the School's technical staff regularly to review data from the filtering system, discuss trends, incidents and new technologies. Filtered terms will be reviewed to check they are proportionate. Checks will be recorded so they can be reviewed. We will record when the checks took place, who did the check, what they tested or checked and resulting actions

We will ensure that:

- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- blocklists are reviewed and they can be modified in line with changes to safeguarding risks

At Nottingham High School:

- web filtering is provided by Smoothwall on school site and, for school devices used in the home, Google Workspace.
- changes can be made by trained members of the IT department.
- overall responsibility is held by the DSL.
- technical support and advice, setup and configuration are from Smoothwall.
- regular checks are made half termly by senior members of the IT department with online safeguarding responsibilities to ensure filtering is still active and functioning everywhere. These are evidenced in monthly reports and recorded actions etc.
- an annual review is carried out as part of the online safety audit to ensure a whole school approach.

14. Students' and Parents' Social Media Presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents and students will use it. However we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, students and parents, also undermining staff morale and the reputation of the school (which is important for the students we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+). We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our students/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use.

Although the school has official social media accounts and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school.

Students are not allowed to contact any staff, governors, volunteers and contractors in order to initiate private communication, such as a DM in Instagram or a direct message in Twitter/X.