Stretford Grammar School

Aspirat primo fortuna labori

Online Safety Policy

Ratified by Governors:September 2025

Date of Review : September 2025

Governing Body Sub-Committee with Reviewing Responsibility: Student Welfare and Admissions

Member of staff with overall responsibility: DSL

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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 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 Headteachers and school staff

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.

Maintained schools and academies that follow the National Curriculum insert:

The Policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher 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 also make sure all staff receive regular online safety updates (via email, and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Governing Body will make sure that the school teaches students how to keep themselves and others safe, including online.

The Governing Body will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's 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 the school's safeguarding needs

The governor who oversees online safety is Mr A Patel

All governors will:

Make sure they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet Appendix 2

Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures

Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for 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

3.2 The Headteacher

The Headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding lead (DSL)

Details of the school's designated safeguarding lead and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

Supporting the Headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school

Working with the Headteacher and Governing Body to review this policy annually and make sure 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

Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly

Working with the Network Manager to make sure the appropriate systems and processes are in place

Working with the Headteacher, Network 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

Responding to safeguarding concerns identified by filtering and monitoring

Making sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy

Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour and Positive Relationship Policy

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 Headteacher and Governing Body

Undertaking annual risk assessments that consider and reflect the risks students face

Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

3.4 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 make sure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

Making sure 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 monthly basis

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy

Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.5 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 (appendix 2), and making sure that students follow the school's terms on acceptable use (appendices 1 and 2)

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 speaking to the DSL or Deputies before they leave. They can be contacted via Reception staff

Following the correct procedures by speaking to the Network Manager if they need to bypass the filtering and monitoring systems for educational purposes. The Network Manager will discuss this with the DSL or Deputies

Working with the DSL to make sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy

Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour and Positive Relationship Policypolicy

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'

3.6 Parents/carers

Parents/carers are expected to:

Notify a member of staff or the Headteacher of any concerns or queries regarding this policy

Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

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

What are the issues? – UK Safer Internet Centre

Help and advice for parents/carers – Childnet

Parents and carers resource sheet – Childnet

3.7 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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. 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 and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for teaching until 31 August 2026).

All schools have to teach:

Relationships and sex education and health education in secondary schools

Primary schools insert:

In Key Stage (KS) 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

In KS3, 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 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, 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 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)

The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online

All schools – adapt this to reflect your school's approach:

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.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website

This policy will also be shared with parents/carers.

Online safety will also be covered during parents' information evenings.

A monthly online safety newsletter will be shared with all parents via email

Regular live and online safety sessions will be shard with parents/carers

The school will let parents/carers know:

What systems the school uses to filter and monitor online use

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 Progress Leader and/or the DSL or Deputies

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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 encourage them to do so, including where they are a witness rather than the target.

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. It will be discussed in form times and assemblies and where the opportunity arises.

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 11 for more detail).

Cyber bullying is included in online safety newsletters and parents are reminded regularly of the reporting systems in school for students and teachers.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and relationship 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.

6.3 Examining electronic devices

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

Poses a risk to staff or students, 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 students and staff. If the search is not urgent, they will seek advice from the Headteacher, DSL or Deputies

Explain to the student why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it

Seek the student's co-operation

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 Headteacher, DSL or Deputies 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 whether 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/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 Deputies 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

Our Behaviour and Positive Relationship Policy

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

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT, CoPilot and Google Gemini

Students are not permitted to use AI in school. Where teachers wish students to have access to AI, they should make a request to the Network Manager so that these may be permitted.

Stretford Grammar School recognises that AI has many uses to help students 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.

Stretford Grammar School will treat any use of AI to bully students very seriously, in line with our Behaviour and Positive Relationship Policy and Anti-Bullying Policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, students and staff.

7. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

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.

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

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in school.

Students may bring mobile devices into school, but they must be switched off and away whilst in school.

Year 7 and 10 students place their mobile phones in secure magnetic-sealed pouches which are sealed and keep phones locked away for the duration of the time spent in school. Students are able to reopen the pouch on their exit from school. We will be moving towards introducing this intervention for all students in the future.

Sixth Form students are permitted to use mobile phones in designated Sixth Form areas.

Where these rules are breached, consequences will be issued in line with the Behaviour and Positive Relationship Policy.

9. 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 can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager

Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

Making sure the device locks if left inactive for a period of time

Not sharing the device among family or friends

Installing anti-virus and anti-spyware software

Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

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 and their line manager

10. 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. 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 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.

11. Training

11.1 Staff, governors and volunteers

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 safeguarding briefings

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

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 child protection and safeguarding policy.

11.2 Students

All students will receive age-appropriate training on safe internet use, including:
Methods that hackers use to trick people into disclosing personal information
Password security
Social engineering
The risks of removable storage devices (e.g. USBs)
Multi-factor authentication
How to report a cyber incident or attack
How to report a personal data breach
Students will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

Staff including DSL and Deputies log behaviour and safeguarding issues related to online safety on CPOMS. Actions are logged by Pastoral Staff and the Safeguarding

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 students 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
Behaviour and Positive Relationship Policy
Staff Disciplinary procedures
Data Protection Policy
Complaints Procedure

Appendix 1: KS2, KS3 and KS4 acceptable use agreement (students and parents/carers)

Adapt this agreement to reflect your school's approach, in line with any changes you made to this policy.

Acceptable use of the school's ICT systems and internet: agreement for students and parents/carers	
Name of student:	
I will read and follow the rules in the acceptable use agreement policy. When I use the school's ICT systems (like computers) and get onto the internet in school I will: Always use the school's ICT systems and the internet responsibly and for educational purposes only Keep my usernames and passwords safe and not share these with others Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others Always log off or shut down a computer when I've finished working on it I will not: Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity Open any attachments in emails, or follow any links in emails, without first checking with a teacher Use any inappropriate language when communicating online, including in emails Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate Log in to the school's network using someone else's details Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision If I bring a personal mobile phone or other personal electronic device into school: I will keep it switched off and out of sight whilst on school property I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (student):	Date:
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	Date:

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Adapt this agreement to reflect your school's approach, in line with any changes you made to this policy.

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) Use them in any way that could harm the school's reputation Access social networking sites or chat rooms Use any improper language when communicating online, including in emails or other messaging services Install any unauthorised software, or connect unauthorised hardware or devices to the school's network Share my password with others or log in to the school's network using someone else's details Take photographs of students without checking with teachers first Share confidential information about the school, its students or staff, or other members of the community Access, modify or share data I'm not authorised to access, modify or share Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the Designated Safeguarding Lead and Network Manager know if a student informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	Date: