Stretford Grammar School

Aspirat primo fortuna labori

Online Safety Policy

Ratified by Governors: December 23

Stretford Grammar School

Aspirat primo fortuna labori

Online Safety Policy

Member of staff responsible: AHT with responsibility for Online Safety
Date: November 2023
Governing Body Sub-Committee with reviewing responsibility: Student Welfare

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- 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, anti-Semitism, 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 scam

2. Legislation and guidance

- This policy is based on the Department for Education's (DfE) 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

  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 pupils' electronic devices where they believe there is a 'good reason' to do so.
- The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board.

- The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). This will take the form of CPOMs reports and cloud based tracking software.
- The governor who oversees online safety is David Wilson.
- All governors will ensure that 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.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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.
- The governing board 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 board 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 those 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.

3.2 The Headteacher

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

3.3 The designated safeguarding lead

(Details of the school's DSL and safeguarding team are set out in our Safeguarding and Child Protection Policy as well as relevant job descriptions.)

The DSL takes lead responsibility for online safety in school (supported by the deputy DSL), 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 headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this policy and the Safeguarding and Child Protection Policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety as required and in line with staff training needs.
- Liaising with other agencies and/or external services if necessary and logging all incidents and actions on CPOMS.
- Provide regular reports on online safety incidents and actions (including any training undertaken) in school to the headteacher and Student Welfare governing board.

3.4 The ICT manager

The ICT manager 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 pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material (Lightspeed Filter & Alert).
- 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 weekly basis.
- Putting into place systems and processes that block access to potentially dangerous sites 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 this policy and the Safeguarding and Child Protection Policy via CPOMS and in liaison with the safeguarding team.
- Ensuring 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 and Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (by reading and signing the school's online AUP), and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this policy and the Safeguarding and Child Protection Policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour 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'

3.6 Parents

Parents are expected to:

- Notify a member of staff, the safeguarding team or the headteacher 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.
- 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 factsheet - Childnet International
    - Healthy relationships – Disrespect Nobody

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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating pupils about online safety

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

All schools will have to teach:

- Relationships and sex education and health education in secondary schools.

In Key Stage 3, 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 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, 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 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.

5. Educating parents about online safety

- The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. Online safety will also be covered during parents' information evenings. These presentations are published on our school website for parents to follow the embedded links.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher, the DSL (or safeguarding team), or the member of the pastoral team with responsibility for the year group. These concerns will be dealt with in line with this policy and the Safeguarding and Child Protection Policy.
- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

- Parents are made aware that the school uses monitoring software called Lightspeed
- Parents are informed about what their child is required to do online through curriculum information on our website.

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 one 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 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, 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. Form Tutors will discuss cyber-bullying with their tutor groups.
- 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 (PSHCE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
- The school also provides up to date information on cyber-bullying to parents so that 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 behaviour 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 ad dealt with in accordance with this policy and the Safeguarding and Child Protection Policy.
- The DSL (liaising with the Safeguarding Team) will consider whether the incident should be reported to the police if it involves illegal material, and will 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 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, the authorised staff member will:
- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil'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 members of the Safeguarding 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 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 pupils 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 policy
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 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.
- Stretford Grammar School 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.
- Stretford Grammar School will treat any use of AI to bully pupils in line with our [anti-bullying/behaviour] 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.

7. Acceptable use of the internet in school

- All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Google Classroom AUP Form). 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in school

- School acknowledges that the use of mobile phones can be a useful tool for safety and contact reasons between parents/carers and their child. Therefore pupils may bring mobile devices to school, but on entering the site they must be switched off and kept securely out of site. Pupils are not permitted to use them during:
  - Lessons
  - Tutor group time
  - Break and lunch time
  - Clubs before or after school, or any other activities organised by the school
- Any use of mobile devices (such as tablets or laptops) in school by pupils must be in line with the acceptable use policy.
- Any breach of the acceptable use policy by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted via bitlocker – 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.
- Keeping operating systems up to date by bringing devices into school when requested so that updates can be installed and the devices maintained (including the installing of anti-virus and anti-spyware software).

- Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in the acceptable use policy (Google Form).
- 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 Network Manager.

10. 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 our policies on Behaviour and the Acceptable Use. 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 code of conduct and the Acceptable Use Policy. 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.

11. 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).
- 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, 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 pupils can recognise dangers and risks in online activity and can weigh the risks up
  - 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 deputy DSL 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.

12. Monitoring arrangements

- The DSL logs behaviour and safeguarding issues related to online safety. Incident report logs can be provided at any time via CPOMS logs and reports and will be routinely produced and discussed at Governor, SLT and staff level as appropriate.
- This policy will be reviewed every year by the DSL/Deputy DSL. At every review, the policy will be shared with the governing board. 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.

STAFF AND GOVERNOR AUP

I agree to the following:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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 which 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

· Share confidential information about the school, its pupils 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 understand that:

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems and that they are monitored by keyword detection at all times and visual threat monitoring.

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 (DSL) and Network Manager know if a pupil informs me they have found any material which 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 pupils in my care do so too.

STUDENT AUP

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
- Only use them when a teacher is present, or with a teacher's permission
- 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 which 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 turn it off upon entering the premises and not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- 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.