Stretford Grammar School

Aspirat primo fortuna labori

Online Safety Policy

Ratified by Governors: TBC

Stretford Grammar School

Aspirat primo fortuna labori

Online Safety Policy

Member of staff responsible: Mr D. Price
Date: February 2021
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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

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 Maureen Brettell.
- 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.

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, 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.
- 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 appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material (SMOOTHWALL, Impero, SENSO).
- 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.
- 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.

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:

Under the new requirement, 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.

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.
- 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.

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 (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 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

- School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
- When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
  - Cause harm, and/or
  - Disrupt teaching, and/or
  - Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

- Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

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).
- 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.