STOCKPORT GRAMMAR SCHOOL

ONLINE SAFETY POLICY

(Approved by Governors October 2025)

Contents

STOCKPORT GRAMMAR SCHOOL

ONLINE SAFETY POLICY

1 Aims

1.1 This is the online safety policy of Stockport Grammar School.

1.2 The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which:

1.2.1 protects the whole School community from illegal, inappropriate and harmful content or contact;

1.2.2 educates the whole School community about their access to and use of technology; and

1.2.3 establishes effective mechanisms to identify, intervene and escalate incidents where appropriate.

2 Scope and application

2.1 This policy applies to the whole School including the Early Years Foundation Stage (**EYFS**).

2.2 This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's technology whether on or off School premises, or otherwise use technology in a way which 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.

3 Regulatory framework

3.1 This policy has been prepared to meet the School's responsibilities under:

3.1.1 Education (Independent School Standards) Regulations 2014;

3.1.2 EYFS statutory framework for group and school-based providers (September 2025);

3.1.3 Education and Skills Act 2008;

3.1.4 Children Act 2004;

3.1.5 Childcare Act 2016;

3.1.6 Data Protection Act 2018 and General Data Protection Regulation (GDPR); and

3.1.7 Equality Act 2010.

3.2 This policy has regard to the following guidance and advice:

3.2.1 Sharing nudes and semi-nudes Advice for Education Settings working with children and young people. Responding to incidents and safeguarding children and young people (UK Council for Internet Safety March 2024);

3.2.2 Keeping Children Safe in Education (DfE, September 2025);

3.2.3 Preventing and tackling bullying (DfE, July 2017);

3.2.4 The Prevent Duty: safeguarding learners vulnerable to radicalisation(Department for Education September 2023) and

3.2.5 Searching, screening and confiscation: advice for schools (DfE, July 2022).

3.3 The following School policies, procedures and resource materials are relevant to this policy:

3.3.1 Acceptable Use Policy for pupils;

3.3.2 Staff IT Acceptable Use Policy and Social Media Policy;

3.3.3 Safeguarding Policy and procedures;

3.3.4 Anti-Bullying Policy;

3.3.5 Risk Assessment Policy for Pupil Welfare;

3.3.6 Staff Code of Conduct (appended to the safeguarding policy) and Protected Disclosure (whistleblowing) policy;

3.3.7 Data Protection Policy for staff;

3.3.8 Information Security Policy (including remote working and bring your own device to work);

4 Publication and availability

4.1 This policy is published on the School website and is available internally on the School's Policy Drive.

4.2 This policy is available in hard copy on request.

4.3 A copy of the policy is available for inspection from the Bursary during the School day.

4.4 This policy can be made available in large print or other accessible format if required.

5 Definitions

5.1 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology**).

6 Responsibility statement and allocation of tasks

6.1 The Governors of the school have overall responsibility for all matters which are the subject of this policy.

6.2 The Governors are required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Governors' response to this duty.

6.3 To ensure the efficient discharge of its responsibilities under this policy, the Governors have allocated the following tasks:

Task	Allocated to	When / frequency of review
Keeping the policy up to date and compliant with the law and best practice	The Bursar	As required, and at least biennially
Review of criteria to be used to determine an incident	Designated Safeguarding Leads (Junior and Senior Schools)	As required, and at least annually
Monitoring the implementation of the policy and evaluating effectiveness	The Head of Digital Services	As required, and at least termly
Online safety	Designated Safeguarding Leads (Junior and Senior Schools)	
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR	The Bursar	As required, and at least termly
Formal annual review	The Governing Body	Bi-annually

7 Role of staff and parents

7.1 Head(s) and Senior Leadership Team

7.1.1 The Head(s) have overall executive responsibility for the safety and welfare of members of the School community.

7.1.2 The Designated Safeguarding Leads are the members of staff from the School's leadership team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the Designated Safeguarding Leads includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the School's child protection and safeguarding policy and procedures.

7.1.3 The Designated Safeguarding Leads will work with the Head of Digital Services (see below) in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

7.1.4 The School has appropriate filtering in place. The Designated Safeguarding Leads will work with the Head of Digital Services to review the effectiveness of the School's web filtering on an annual basis. The Head of Digital Services will also perform a termly test of effectiveness.

7.1.5 The School uses an email key-word monitoring system for pupil and staff emails. Any emails containing a key word are held for approval from a senior member of staff before being delivered.

7.1.6 The School has appropriate pupil monitoring in place. This monitoring alerts necessary staff members when any digital activity reaches a safeguarding

concern threshold. Records are kept of all serious incidents involving the use of technology and, where necessary, incidents are followed up as per the School's safeguarding policy.

7.2 **Head of Digital Services**

7.2.1 The Head of Digital Services is responsible for ensuring that:

(a) the School's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

(b) the user may only use the School's technology if they are properly authenticated and authorised;

(c) the School has effective filtering , monitoring and email key word detection systems in place;

(d) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised; and

(e) the use of the School's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation;

7.2.2 If the Head of Digital Services has concerns about the functionality, effectiveness, suitability or use of technology within the School, with regards to the filtering and monitoring systems in place, they will escalate those concerns promptly to the Designated Safeguarding Leads.

All staff

7.2.3 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the School's policies and of safe practice with the pupils.

7.2.4 Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

7.2.5 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's child safeguarding policy and procedures.

7.3 **Parents**

7.3.1 The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. The School expects parents to promote safe practice when using technology and to:

(a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

7.3.2 If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Leads.

8 Access to the School's technology

8.1 The School provides internet, intranet access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective acceptable use policy when using School technology. In the Junior School, access by children is monitored by an adult at all times.

8.2 Pupils and staff require individual usernames and passwords to access the School's internet, intranet and email system which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their usernames or passwords must report it to the ICT team

8.3 The School has separate Wi-Fi connections available for use by staff, sixth form pupils and visitors to the School. Access to these connections is based on school user credentials or a secure password for visitors.

8.4 Use of mobile electronic devices

8.4.1 Mobile devices equipped with a mobile data subscription can provide pupils with unlimited and unrestricted access to the internet.

8.4.2 The School rules about the use of mobile electronic devices, including access to open / non-School networks, are set out in the acceptable use policy for pupils.

8.4.3 The School's policies apply to the use of technology by staff and pupils 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.

9 Procedures for dealing with incidents of misuse

9.1 Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

9.2 Misuse by pupils

9.2.1 Anyone who has any concern about the misuse of technology by pupils should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the anti-bullying policy where there is an allegation of cyberbullying.

9.2.2 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's safeguarding procedures (see the School's Safeguarding Policy and procedures).

9.3 Misuse by staff

9.3.1 Anyone who has any concern about the misuse of technology by staff should report it in accordance with the School's Protected Disclosure (whistleblowing) Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

9.3.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they should be report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding Policy and procedures.

9.4 **Misuse by any user**

9.4.1 Anyone who has a concern about the misuse of technology by any other user should report it immediately to the Head of Digital Services, the Network Manager or the Designated Safeguarding Lead.

9.4.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

9.4.3 If the School considers that any person is vulnerable to radicalisation the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

10 Education

10.1 The safe use of technology is integral to the School's curriculum. Pupils are educated in an age-appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices (see the School's Curriculum Policy).

10.2 Technology is included in the educational programmes followed in the EYFS in the following ways:

10.2.1 children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

10.2.2 children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

10.2.3 children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

10.3 The safe use of technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial / pastoral activities, teaching pupils:

10.3.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

10.3.2 to be critically aware of content they access online and guided to validate accuracy of information;

10.3.3 how to recognise suspicious, bullying or extremist behaviour;

10.3.4 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

10.3.5 the consequences of negative online behaviour; and

10.3.6 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

10.4 The safe use of technology aspects of the curriculum are reviewed on a regular basis to ensure their relevance.

10.5 The School's acceptable use policy for pupils sets out the School rules about the use of technology, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy or, for younger children, the principles of the policy, on a regular basis.

11 Training

11.1 Staff

11.1.1 The School provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.

11.1.2 Inductions for new staff cover the Staff Code of Conduct and Staff IT Acceptable Use Policy. Ongoing staff development training includes training on technology safety together with specific safeguarding issues.

11.1.3 Staff also receive data protection training on induction and at regular intervals afterwards.

11.1.4 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

Parents

11.1.5 The School aims to inform, communicate with and educate parents in the safe use of technology through interactive engagement with relevant online safety resources, information evenings and newsletter updates.

11.1.6 Parents are asked to read the acceptable use policy for pupils with their son / daughter to ensure that it is fully understood.

12 Risk assessment

12.1 Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

12.2 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

12.3 The Heads have overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

13 Record keeping

13.1 All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

13.2 The records created in accordance with this policy may contain personal data. The School has a number of privacy notices which explain how the School will use personal data about pupils and parents. The privacy notices are published on the School's website. In addition, staff must ensure that they follow the School's data protection policies and procedures when handling personal data created in connection with this policy. This includes the School's Data Protection Policy and Information Security policies.

STOCKPORT GRAMMAR SCHOOL

ONLINE SAFETY POLICY – APPENDIX

Context

This is an appendix to the School's Online Safety Policy, IT Acceptable Use Policy for Staff, IT Acceptable Use Agreement for Pupils, Data Protection Policy and Information Security Policy. This appendix summarises key changes or additions during remote learning.

We will continue to ensure that appropriate filters and monitoring systems are in place to protect pupils when they are online on our IT systems or recommended resources.

The person in charge of maintaining safe IT arrangements in the School is Mr A Kershaw and he can be contacted by email on ictcoordinator@stockportgrammar.co.uk

Should the School's IT staff become unavailable, we will publish contingency arrangements to ensure the safety and stability of our IT provision.

Pupils should continue to follow our normal policies and procedures whether working in school or remotely at home.

1 Remote learning arrangements

The same principles as set out in the School's Safeguarding Policy and Pupil Behaviour and Discipline Policy apply to all online interactions between staff and pupils.

Appendix 2 of the School's Safeguarding Policy (Staff Code of Conduct) already includes provision relating to staff/pupil relationships and communication using technology. This Code of Conduct also applies to remote learning.

Remote learning will be delivered via the following platforms/facilities which have been evaluated and agreed by the School's Senior Management Team:

- Frog
- Google Classroom
- Google Meet (live and recorded)
- Microsoft 365
- Canva
- Tapestry
- School email accounts

Staff, pupils and parents will be sent advice and guidance on remote learning as appropriate.

2 Online safety arrangements for pupils in school during a school closure

Pupils in school will work on the same tasks as pupils working remotely using the same platforms/facilities and will be supervised by a member of staff.

3 Role of parents

Parents have responsibility for ensuring appropriate supervision when their children are working online and that appropriate online parent controls are in place.

The following are suitable online safety resources for parents:

- Thinkuknow provides advice from the National Crime Agency (NCA) on staying safe online
- Parent info is a collaboration between Parent Zone and the NCA providing support and guidance for parents from leading experts and organisations
- Childnet toolkit is a toolkit to support parents to start discussions about online behaviour
- UK Safer Internet Centre has advice for parents to help keep children safe online
- Internet matters provides guides on how to set parental controls on a range of devices
- Net-aware has guides for parents on social networks, apps and games
- London Grid for Learning has support for parents to keep their children safe online
- Let's Talk About It has advice for parents to keep children safe from online radicalisation

4 Safeguarding arrangements

The School's arrangements for reporting safeguarding concerns are set out in the School's Safeguarding Policy.

Pupils and parents can also access help and support at:

- UK Safer Internet Centre 'Report Harmful Content' to report harmful content
- CEOP (National Crime Agency Child Exploitation and Online Protection Command to report online abuse
- Educate Against Hate for government advice on safeguarding from radicalisation

5 Staff training

Staff have been given training on the use of the online platforms/facilities that the school uses. Updates to this training are provided as necessary.

Authorised by **Chair of Governors**	
Date	14.10.2025

Circulation	Governors / teaching staff / all staff / parents / website
Status	Regulatory