

Greenfields Community School

Online Safety Policy



September 2026

Document Origins		
Version Date	Review date	Approval date
September 2024	September 2025	FGB 1/10/24
September 2025	September 2026	FGB 9/12/25
September 2026	September 2027	FGB

Document Version History		
Revision date	Author of changes	Summary of changes
September 2025	L. Maltby	Update of previous version
September 2026	L. Maltby	Comprehensive update of title, content and procedures in line with Keeping Children Safe in Education, Online Safety Act updates 2026 and school procedures.

1. Aims

Greenfields Community School is committed to safeguarding and promoting the welfare of children and recognises that online safety is an essential component of safeguarding.

The school seeks to provide pupils with access to technology and online resources that support learning while ensuring they are protected from harm. The school recognises that the internet, mobile technologies, online communication platforms and emerging technologies, including Artificial Intelligence (AI), present both opportunities and risks.

This policy aims to:

- Safeguard pupils and staff when using digital technologies.
- Promote safe, responsible and respectful online behaviour.
- Ensure compliance with safeguarding and data protection legislation.
- Protect children from inappropriate content, contact, conduct and commercial risks online.
- Establish clear procedures for responding to online safety concerns.
- Support pupils, staff, governors and parents in understanding their online safety responsibilities.
- Ensure appropriate filtering and monitoring systems are in place to protect pupils. This aligns with Department for Education expectations for schools.

2. Relevant Legislation and Guidance

This policy should be read alongside:

- Keeping Children Safe in Education 2026 (DfE).
- Working Together to Safeguard Children.
- Education for a Connected World (UK Council for Internet Safety).
- Meeting Digital and Technology Standards in Schools and Colleges.
- UK GDPR.
- Data Protection Act 2018.
- Prevent Duty Guidance.
- School Safeguarding and Child Protection Policy.

- Filtering and Monitoring Policy.
 - Behaviour Policy.
 - Staff Code of Conduct.
 - Acceptable Use Agreements.
-

3. Roles and Responsibilities

3.1 Governing Body

The Governing Body will:

- Ensure appropriate filtering and monitoring systems are in place.
- Regularly review online safety arrangements.
- Monitor the effectiveness of this policy.
- Ensure staff receive appropriate safeguarding and online safety training.

3.2 Headteacher

The Headteacher will:

- Lead on implementation of this policy.
- Ensure online safety is embedded within safeguarding arrangements.
- Ensure concerns are acted upon appropriately.
- Ensure all staff understand their responsibilities.

3.3 Designated Safeguarding Lead (DSL)

The DSL will:

- Take lead responsibility for online safeguarding.
- Understand filtering and monitoring systems used by the school.
- Respond to online safety incidents.
- Maintain records of concerns and actions taken.
- Liaise with external agencies where necessary.

3.4 Staff

All staff must:

- Promote safe online behaviour.
- Monitor pupils' use of technology.

- Report concerns immediately to the DSL.
- Follow the Staff Code of Conduct and Acceptable Use Policy.
- Complete regular safeguarding and online safety training.

3.5 Pupils

Pupils are expected to:

- Use technology responsibly.
- Follow school Acceptable Use Agreements.
- Respect others online.
- Report anything that makes them feel uncomfortable, unsafe or worried.

3.6 Parents and Carers

Parents and carers are encouraged to:

- Support online safety messages at home.
- Monitor their child's online activity appropriately.
- Report concerns to the school.
- Engage with school online safety information sessions and resources.

4. Online Safety Education

Online safety education will be delivered through:

- Computing lessons using Purple Mash
- RSHE lessons using Jigsaw
- Assemblies.
- Safeguarding activities.
- Anti-bullying initiatives.
- Safer Internet Day activities.

Teaching will reflect the strands within Education for a Connected World, including:

- Self-image and identity.
- Online relationships.
- Online reputation.
- Online bullying.
- Managing online information.

- Health, wellbeing and lifestyle.
- Privacy and security.
- Copyright and ownership.

Pupils will learn:

- How to stay safe online.
- How to recognise harmful content.
- How to identify misinformation and disinformation.
- How to protect personal information.
- How to report concerns.
- How to recognise online scams and phishing attempts.
- How to use AI safely and responsibly.

5. Acceptable Use of Technology

All users of school technology must:

- Access only approved resources.
- Use technology for educational purposes.
- Respect the privacy and rights of others.
- Protect passwords and account details.
- Not attempt to bypass filtering or monitoring systems.
- Not engage in illegal, harmful or inappropriate activity.

Unauthorised access to computer systems may constitute an offence under the Computer Misuse Act 1990.

Please see Acceptable Use Policy GCS 2024 Update 2025

6. Internet Access

The school will provide supervised access to online resources.

- Internet use will support teaching, learning and administration.
- Pupils will receive age-appropriate supervision.
- Parents will be informed that pupils access online resources in school.
- Pupils and parents will sign Acceptable Use Agreements.

- Internet use may be monitored for safeguarding and security purposes.
-

7. Filtering and Monitoring

The school operates filtering and monitoring systems to reduce the likelihood of pupils accessing harmful material and to identify potential safeguarding concerns.

Filtering systems will:

- Block illegal content.
- Restrict access to inappropriate content.
- Be age-appropriate.
- Be reviewed regularly.
- Include protection against emerging online risks and AI-generated content where appropriate.

Monitoring systems will:

- Identify potentially harmful online activity.
- Support safeguarding investigations.
- Generate alerts where appropriate.
- Be reviewed regularly to ensure effectiveness.

The Headteacher, DSL, Governors and IT support provider will review filtering and monitoring arrangements annually, or sooner where necessary.

If unsuitable material is identified:

- Access should cease immediately.
- The incident should be reported to the DSL and Headteacher.
- Appropriate safeguarding procedures will be followed.
- Illegal content will be reported to relevant authorities where required.

Please see Filtering and Monitoring Policy GCS Sept 2026

8. Social Media

The school recognises that social media forms part of modern life.

Staff must:

- Maintain professional boundaries.

- Not communicate with pupils through personal social media accounts.
- Follow the Staff Code of Conduct.
- Protect their professional reputation online.

Pupils will be taught:

- Safe and respectful social media use.
- How to manage privacy settings.
- How to report concerns.
- How online behaviour can affect future opportunities.

9. Artificial Intelligence (AI)

The school recognises the increasing use of AI tools within education.

Staff and pupils must:

- Use AI safely, responsibly and ethically.
- Verify information generated by AI before use.
- Not enter personal, confidential or sensitive information into AI systems.
- Not use AI to facilitate cheating, plagiarism or harmful behaviour.
- Follow school guidance regarding approved AI platforms.

Staff remain responsible for all content used within teaching and learning.

Please see AI Policy GCS Feb 2026

10. Cyberbullying

Cyberbullying is unacceptable and will be addressed in line with the school's Behaviour and Anti-Bullying Policies.

Examples include:

- Sending offensive or threatening messages.
- Sharing harmful content.
- Harassment through social media.
- Excluding others intentionally online.
- Impersonating others online.

The school will:

- Investigate incidents promptly.
 - Retain evidence where appropriate.
 - Support victims.
 - Apply sanctions where necessary.
 - Involve parents and carers.
 - Contact external agencies or police where appropriate.
-

11. Personal Data and Images

The school will comply with UK GDPR and the Data Protection Act 2018.

- Images of pupils will only be used in accordance with parental consent preferences.
 - Personal information will not be published without appropriate authorisation.
 - Staff and pupils must protect confidential information.
 - Any data breach will be reported in accordance with school procedures.
-

12. Mobile Phones, Smart Devices and Mobile Technology

Greenfields Community School is committed to providing a safe, calm and focused learning environment. In line with the Department for Education's statutory guidance on mobile phones in schools, the school operates as a mobile phone-free environment by default.

12.1 Pupil Use of Mobile Phones and Smart Devices

- Pupils are not permitted to use mobile phones during the school day.
- The prohibition applies to mobile phones and other smart devices with similar functionality, including smart watches and devices capable of sending or receiving messages, accessing the internet, receiving notifications, or recording images, audio or video.
- Any exceptions will be considered on an individual basis where required to support a pupil's medical, safeguarding or special educational needs.
- Pupils bringing mobile phones onto the school site must follow the school's Mobile Phone Procedures and any storage arrangements implemented by the school.

12.2 Use of Mobile Technology

- Mobile phones, smart watches and other recording-enabled devices must not be used to take photographs, videos or audio recordings without the explicit permission of a member of staff.
- Mobile devices must not be used to bully, intimidate, harass or cause distress to others.
- Pupils must not share personal information, images or videos of other members of the school community without appropriate consent.

12.3 Staff Use of Mobile Devices

- Staff must use mobile devices in accordance with the Staff Code of Conduct and Data Protection policies.
- Personal devices must not be used to communicate with pupils or parents unless authorised through approved school systems.
- Confidential, safeguarding or personal information must only be accessed, stored or shared using approved and secure school systems.

12.4 Breaches of this Policy

- Parents/carers may be informed of serious breaches.
- Misuse involving safeguarding concerns, cyberbullying, inappropriate images, online harassment or criminal activity will be referred to the Designated Safeguarding Lead (DSL) and, where appropriate, external agencies including the police.

12.5 Monitoring and Review

The school will regularly review its mobile phone and smart device arrangements to ensure continued compliance with statutory guidance, safeguarding requirements and the needs of the school community. The effectiveness of the school's mobile phone policy will be monitored by senior leaders and governors

13. Reporting Concerns

All online safety concerns must be reported immediately.

Concerns may include:

- Inappropriate content.
- Cyberbullying.
- Online grooming concerns.
- Radicalisation concerns.
- Sextortion or exploitation concerns.

- Malware or cyber security incidents.
- Access to illegal content.

Staff must report concerns to the DSL without delay and log concerns on My Concern.

Where necessary, referrals may be made to:

- Children's Social Care.
 - Police.
 - CEOP.
 - Local Authority Safeguarding Partners.
 - Other relevant agencies.
-

14. Staff Training

All staff will receive:

- Annual safeguarding training.
 - Regular online safety updates.
 - Information about emerging technologies and risks.
 - Guidance on filtering and monitoring arrangements.
 - Cyber security awareness training.
-

15. Monitoring and Review

This policy will be reviewed annually by the Headteacher, DSL and Governing Body, or sooner if required by:

- Legislative changes.
- Changes to safeguarding guidance.
- Significant online safety incidents.
- Developments in technology.

The Governing Body will monitor the implementation and effectiveness of this policy on an ongoing basis.