Online Safety Policy 2026-2027

Document Information	
Policy Owner	Headteacher: Mrs Sarah Allen
Policy Writer	Headteacher: Mrs Sarah Allen
Approval Body	Ascent Academy Trust Board
Date Approved	September 2026
Review Date	September 2027
Version	2.0 - aligning with all new Digital and Cyber Security Policies for 2026-2027
Statutory	Yes
Applies to:	Whole School

Approval

Role	Name	Signature	Date
Headteacher	S. Allen		August 2026
Chair of Governors/Trustees	K. Hermon P. Hill (Chair of Trustees)		
Policy Writer	S. Allen		August 2026

c/o The Woodsetton School, Tipton Road, Dudley, West Midlands DY3 1BY

Tel: 01384 818265 Email: info@woodsetton.dudley.sch.uk

1. Introduction

At Woodsetton School, we are committed to safeguarding and promoting the welfare of all pupils. We recognise that digital technologies and online communication provide significant opportunities for learning, communication, creativity and independence. We also recognise that children and young people can face risks online which may affect their safety, wellbeing and development.

We recognise that many of our pupils may be more vulnerable to online harm due to their special educational needs and disabilities (SEND). Online safety is therefore viewed as an integral part of safeguarding and child protection.

This policy should be read alongside the:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Artificial Intelligence Policy
- Staff Code of Conduct
- Data Protection Policy
- Acceptable Use Agreements
- Remote Learning Policy
- Mobile Phone and Smart Devices Policy
- Safeguarding within the School Curriculum Policy

Definition of Online Safety

Online safety refers to the protection of children, young people and adults in the digital environment. It encompasses not only the safe use of technology, internet-enabled devices and online services, but also the behaviours, attitudes and safeguarding measures required to prevent harm, abuse, exploitation and criminal activity online.

At Woodsetton School, online safety is recognised as a core safeguarding responsibility.

Legal Framework

This policy has regard to:

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children 2026
- Education Act 2002
- Education Act 2011
- UK GDPR
- Data Protection Act 2018
- DfE Teaching Online Safety in Schools Guidance
- DfE Filtering and Monitoring Standards

2. Policy Aims

This policy aims to:

- Safeguard pupils and staff when using digital technologies.
- Promote safe and responsible online behaviours.
- Protect pupils from online abuse, exploitation and harmful content.
- Support pupils in developing age-appropriate digital resilience.
- Ensure staff understand their safeguarding responsibilities.
- Provide a consistent approach to responding to online safety concerns.
- Support parents and carers in promoting online safety at home.

3. Scope

This policy applies to:

- Pupils
- Staff
- Volunteers
- Governors
- Contractors
- Visitors

The policy applies when using:

- School devices
- Personal devices on school premises
- School networks
- Online services provided by the school
- Remote learning platforms
- Online activities that may impact school safeguarding concerns

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, 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 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 scams.

At Woodsetton School, a whole school approach is taken to online safety. We endeavour to ensure appropriate filters and appropriate monitoring systems are in place. Our Children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through personal, social, health and economic education (PSHE) and Relationships, Sex and Health Education (RSHE).

As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material.

Guidance: Teaching Online Safety in schools 2023 Teaching online safety in schools - GOV.UK (www.gov.uk)

4. Understanding Vulnerability in a Special School Context

We recognise that some pupils may:

- Be more trusting of strangers online.
- Have difficulty recognising risk.
- Communicate differently.
- Be vulnerable to manipulation or coercion.
- Have limited understanding of privacy settings.
- Be more likely to overshare personal information.

- Experience difficulties understanding social boundaries.
- Be vulnerable to online bullying, grooming, exploitation or financial scams.
- Require additional support to understand online safety messages.

Additional vulnerabilities may arise from:

- Communication difficulties.
- Social communication needs.
- Difficulties understanding social cues and intent.
- Impulsive behaviours.
- Sensory-seeking behaviours.
- Reduced understanding of privacy and consent.
- Dependency upon online friendships and relationships.
- Limited understanding of commercial exploitation and scams.

Staff will take account of developmental age, communication needs and cognitive understanding when delivering online safety education and managing concerns.

5. Roles and Responsibilities

Governing Body

The Governing Body will:

- Ensure appropriate online safety arrangements are in place.
- Monitor safeguarding and online safety effectiveness.
- Ensure policies are reviewed regularly.
- Support the allocation of resources for online safety measures.
- Ensure the school meets the DfE Filtering and Monitoring Standards and receives assurance regarding their effectiveness.

Governors and trustees will receive appropriate online safety awareness training relevant to their role.

Headteacher

The Headteacher will:

- Ensure this policy is implemented consistently.
- Promote a culture where online safety is recognised as a safeguarding priority.
- Ensure staff receive appropriate training.

Designated Safeguarding Lead (DSL)

The DSL will:

- Lead on online safety safeguarding matters.
- Respond to online safety concerns and incidents.
- Make referrals to external agencies when required.
- Support staff and families.
- Monitor trends and emerging risks.
- Maintain an up-to-date understanding of filtering and monitoring systems and how concerns are escalated and managed.
-

Staff

All staff will:

- Maintain professional online conduct.
- Follow school policies and acceptable use agreements.
- Teach online safety where appropriate.
- Identify and report safeguarding concerns promptly.
- Understand the additional vulnerabilities of SEND pupils online.

All staff receive online safety training as part of induction and regular safeguarding updates.

Training will include:

- Current online risks.
- Filtering and monitoring.
- Online exploitation.
- Professional conduct online.
- Artificial intelligence risks.
- Emerging technologies.

Pupils

Pupils will be supported to:

- Use devices safely and responsibly.
- Treat others respectfully online.
- Seek help when concerned.
- Report online behaviours or content that make them uncomfortable or unsafe.

The school will support pupils, parents and staff in accessing specialist support, including CEOP (Child Exploitation and Online Protection Command), where appropriate.

6. Online Safety Education

Online safety education will be embedded throughout the curriculum and adapted to meet pupils' developmental stage and individual needs.

Teaching may include:

EYFS

- Taking turns with technology.
- Asking trusted adults for help.
- Understanding that not everyone online is known to us.
- Basic personal information awareness.

Primary

- Safe searching.
- Kind online behaviour.
- Cyberbullying awareness.
- Personal information and privacy.
- Trusted adults and reporting concerns.

Methods may include:

- Visual supports
- Social stories
- Symbol-supported resources
- Structured discussion
- Scenario-based learning
- Repetition and reinforcement

7. Filtering and Monitoring

The Governing Body and Headteacher ensure that appropriate filtering and monitoring systems are in place and regularly reviewed. The DSL takes lead responsibility for understanding filtering and monitoring systems and responding to safeguarding concerns identified through them.

Filtering and monitoring support safeguarding but do not replace staff vigilance, supervision and professional curiosity.

A member of the Senior Leadership Team and the DSL receive regular reports regarding filtering and monitoring systems.

Governors/Trustees receive periodic assurance reports regarding the effectiveness of filtering and monitoring arrangements.

The school uses filtering and monitoring systems to help safeguard users.
These systems aim to:

- Restrict access to inappropriate content.
- Identify potential safeguarding concerns.
- Support compliance with safeguarding requirements.

The school recognises that no filtering system can be completely effective and therefore combines technology with education, supervision and safeguarding procedures.

8. Artificial Intelligence (AI)

The school recognises that AI technologies are increasingly accessible and create both educational opportunities and safeguarding risks.
Risks may include:

- Deepfakes and manipulated imagery
- Sharing of nude or semi-nude images
- Image-based abuse
- AI-generated misinformation
- Online impersonation
- Exploitation through AI-enabled communication

Any concerns involving AI-generated content will be treated as safeguarding concerns and managed in accordance with safeguarding procedures. Staff and pupils must not enter confidential or personal information into public AI platforms.

9. Cyber Security

The school recognises that cyber security is an essential component of safeguarding and business continuity.
Staff are expected to:

- Use strong passwords.
- Enable multi-factor authentication where available.
- Report suspicious emails immediately.
- Follow data protection requirements.
- Keep devices secure.

Cyber security incidents will be reported and managed in accordance with the Trust's Cyber Security Policy and Incident Response Procedures.

10. Safeguarding

The school will respond to all online safety incidents proportionately and in accordance with safeguarding procedures.
Responses may include:

- Immediate safeguarding action.
- Risk assessments.
- Engagement with parents and carers.
- Behavioural support strategies.
- Referral to Children's Social Care.
- Referral to Police where criminal offences are suspected.
- Referral to CEOP.

All incidents will be recorded in accordance with safeguarding procedures.

11. Cyberbullying

The school does not tolerate bullying in any form, including online bullying.
Examples include:

- Sending threatening messages.
- Excluding others online.
- Sharing images without consent.
- Posting abusive comments.
- Impersonating others online.

Incidents will be managed in accordance with the Behaviour and Anti-Bullying Policies.

12. Online Abuse and Exploitation

The school recognises the risks associated with:

- Grooming
- Sexual exploitation
- Criminal exploitation
- Radicalisation
- Extremist content
- Harmful online challenges
- Coercion and manipulation
- Sextortion
- Financial exploitation

Any concerns will be treated as safeguarding concerns and dealt with immediately.
Staff **must not** view, download, copy, print, save or share nude or semi-nude images and must immediately refer concerns to the DSL.

The school recognises that incidents involving the consensual or non-consensual sharing of nude and semi-nude images may occur.

Such incidents will never be viewed solely as a behaviour issue and will be managed in line with:

- Keeping Children Safe in Education
- Sharing Nudes and Semi-Nudes Guidance
- Child Protection and Safeguarding Procedures

Appropriate safeguarding support will be provided to all children involved.

13. Use of Images and Videos

The school will:

- Obtain appropriate permissions for photographs and videos.
- Store images securely.
- Ensure images are used appropriately.
- Support pupils in understanding safe image sharing.

Pupils must not photograph or record others without permission.

14. Mobile Phones and Personal Devices

The use of mobile phones and smart devices is governed by the Mobile Phones and Smart Devices Policy. Any safeguarding concerns involving devices will be managed in accordance with the Searching, Screening, Confiscation and Electronic Device Searches Policy.
The school will:

- Restrict device use during the school day.
- Monitor use where appropriate.
- Investigate safeguarding concerns involving personal devices when necessary.

15. Acceptable Use

All users must:

- Use technology responsibly.
- Respect others online.
- Keep passwords secure.
- Report concerns promptly.
- Follow school rules and guidance.

Separate Acceptable Use Agreements will be signed by staff and, where appropriate, pupils and parents.

16. Working with Parents and Carers

Parents and carers play a vital role in supporting online safety.

The school will:

- Provide information and guidance.
- Share emerging online risks.
- Offer support where concerns arise.
- Encourage consistent online safety messages between home and school.

17. Reporting Concerns

All online safety concerns must be reported immediately.

Concerns may include:

- Cyberbullying
- Inappropriate content
- Online exploitation
- Excessive online behaviour
- Harmful contact from others
- Unsafe image sharing
- Online abuse

Staff must report concerns to the DSL in accordance with safeguarding procedures.

18. Monitoring and Review

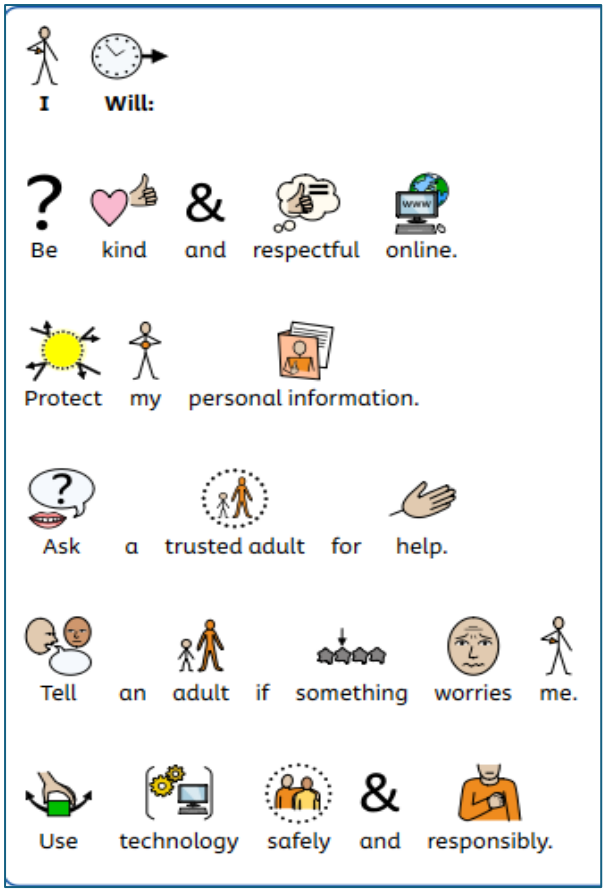
This policy will be reviewed annually or sooner if:

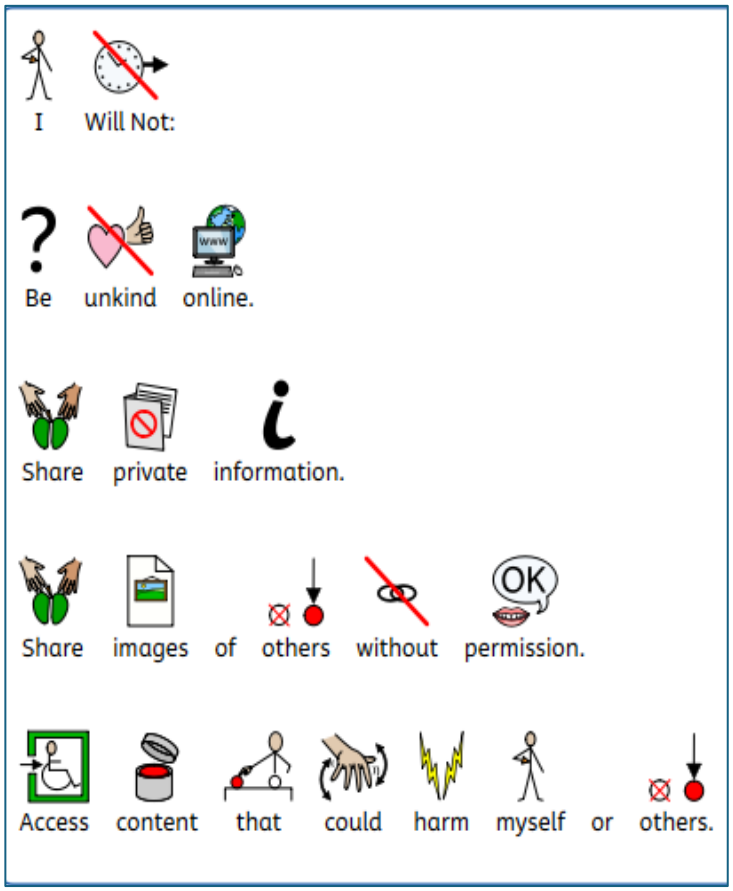
- There are changes to legislation or guidance.
- New technologies create emerging risks.
- Significant incidents identify a need for review.

Rules for Responsible Internet Use - Pupils

At Woodsetton School we encourage the safe use of digital technology including the use of the internet to support learning. In order to safeguard everyone involved we ask pupils to follow the following rules.

I agree to use the internet safely, thinking about what I do, the type of words I use and how I behave online. I know that if I see or read something that makes me feel uncomfortable, then I will tell a trusted adult.





I am aware of the CEOP report button and know when to use it.

CEOP REPORT
ceop.police.uk

I know that anything I share online may be monitored / seen by someone else.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Head/Deputy Head Teacher Signed:

Date:

Pupil Signed:

Date:

Staff Acceptable Use Agreement (AUA)

Responsible Use of Technology, Internet, AI and School Systems

This agreement applies to all staff, governors, volunteers, students, agency staff, contractors and anyone authorised to access Woodsetton School's ICT systems.

The school expects all users to act professionally, responsibly and in accordance with safeguarding, data protection and professional standards at all times. School systems are provided primarily for educational and business purposes and all use must support the safe operation of the school.
Use of school systems may be monitored.

I Will:

Safeguarding and Professional Conduct

- Safeguard the welfare, privacy and dignity of all pupils.
- Maintain professional boundaries at all times.
- Report any online safety, safeguarding or cyber-security concerns immediately to the DSL, Deputy DSL or a senior leader.
- Follow the Safeguarding and Child Protection Policy, Staff Code of Conduct, Online Safety Policy, Mobile Devices Policy and AI Policy.

Use of School Systems

- Use school accounts, systems and devices responsibly and professionally.
- Keep my passwords secure and never share them.
- Log out of systems when not in use.
- Follow copyright and intellectual property requirements.
- Only install software or applications that have been approved by the school.

Data Protection

- Keep personal and confidential information secure.
- Only access information that I need for my role.
- Use approved school systems when handling personal data.
- Ensure personal data is not shared, lost or accessed by unauthorised individuals.
- Follow all GDPR and Data Protection requirements.

Artificial Intelligence (AI)

- Use AI tools responsibly, ethically and professionally.
- Never enter personal, safeguarding-sensitive, confidential or commercially sensitive information into public AI systems.
- Check and verify any AI-generated content before using it.
- Remain accountable for all content, decisions and communications supported by AI.
- Report concerns relating to deepfakes, AI-generated abuse, impersonation or manipulated content.
-

Communication

- Use only approved school communication systems for contact with pupils and families.
- Ensure all communications are professional, appropriate and relate to school business.
- Use school email accounts when communicating on behalf of the school.
- Follow agreed protocols for remote working and online meetings.

I Will Not:

Safeguarding

- Use personal devices to communicate directly with pupils.
- Take photographs, videos or audio recordings of pupils using personal devices.
- Store pupil images or information on personal devices.
- Access, create, possess or share inappropriate, offensive, extremist or illegal content.
- Engage in online behaviour which could bring the school into disrepute.

Security

- Attempt to bypass security, filtering or monitoring systems.
- Access information that I am not authorised to view.
- Share usernames or passwords.
- Download unauthorised software or applications.
- Introduce malicious software or deliberately compromise school systems.

Social Media

- Accept friend requests or follow requests from current pupils on personal social media accounts.
- Discuss pupils, parents, colleagues or confidential school matters online.
- Present personal opinions as representing the views of the school.
- Publish content that could damage professional relationships or the reputation of the school.

Artificial Intelligence

- Use AI to create, share or possess deepfake, nudification or manipulated images involving pupils.
- Use AI-generated content without professional review.
- Upload personal, confidential or safeguarding-related information to public AI platforms.

Monitoring

Staff should be aware that school systems, internet usage, email, cloud services and network activity may be monitored, filtered and reviewed where necessary to protect pupils, staff and the school community and to meet safeguarding, legal and security obligations.

Declaration

I have read, understood and agree to comply with this Staff Acceptable Use Agreement and all associated school policies.
I understand that failure to comply may result in the withdrawal of system access, safeguarding action, disciplinary procedures and/or referral to external agencies where appropriate.

Name: _____

Role: _____

Signature: _____

Date: _____

Manager Signature: _____

Date: _____