



Online Safety Policy

Policy Number	EDE/POL/009	Issue Date	01/09/2025
Issue Number	006	Author	James Madine
School	Acorns School	Approver	Jo Sharpe
Headteacher	Paula Tankard	Designated Safeguarding Lead	Molly McCann

1. Introduction and Context

Keys Group is committed to providing a safe, supportive, and empowering environment for all pupils, including those with complex needs, emotional and behavioural difficulties, or challenging behaviours. Our online safety policy recognises the unique vulnerabilities of our pupils, many of whom have experienced exclusion or trauma, and prioritises safeguarding them from online risks while enabling positive and educational use of technology.

2. Policy Aims

- Ensure robust online safety processes that protect pupils, staff, volunteers, and governors.
- Identify and support pupils who may be at greater risk of harm online.
- Deliver an effective, flexible, and adaptive approach to online safety education tailored to individual pupil needs.
- Establish clear mechanisms for identifying, intervening in, and escalating online safety incidents.
- Provide training and resources that empower staff to support pupils' safe use of technology.

3. Key Online Risks Addressed

Our approach addresses risks under four categories:

- **Content:** Exposure to harmful or inappropriate material including extremist content, self-harm, or misinformation.
- **Contact:** Harmful interactions such as grooming, peer pressure, or exploitation.
- **Conduct:** Risky personal behaviour online including cyberbullying, sharing of explicit images, or misuse of social media.
- **Commerce:** Risks such as online scams, gambling, or inappropriate advertising.

4. Legislative and Regulatory Framework

This policy aligns with:-

- The OFSTED Inspection Toolkit for Non-Association Independent Schools.
- Department for Education statutory guidance including Keeping Children Safe in Education 2025.



- Education Act 1996, Education and Inspections Act 2006, Equality Act 2010.
- UK Council for Internet Safety (UKCIS) guidance.
- Relevant safeguarding and child protection legislation.

5. Roles and Responsibilities

5.1 Governing Body

- Monitor policy implementation and hold leadership to account.
- Ensure staff receive regular online safety training and updates.
- Oversee filtering and monitoring systems and review their effectiveness annually.
- Ensure online safety education is embedded and adapted for pupils with SEND or vulnerabilities.

5.2 Headteacher / School Leader

- Ensure consistent implementation of the policy.
- Lead on online safety culture within the school.
- The school will provide regular communications and training opportunities for parents and carers to support safe and responsible technology use at home.

5.3 Designated Safeguarding Lead (DSL)

- Lead responsibility for online safety incidents and training.
- Oversee filtering and monitoring systems with IT support.
- Log and respond to online safety incidents in line with safeguarding procedures.
- Liaise with external agencies as necessary.

5.4 IT Department

- Maintain secure filtering and monitoring systems tailored to the needs of special school pupils.
- Regularly update security measures and report attempts to access harmful content.
- Support DSL investigations with technical expertise.

5.5 All Staff and Volunteers

- Understand and implement the policy consistently.
- Report online safety concerns promptly.
- Support pupils in safe use of technology, respecting their individual needs.

5.6 Parents/Carers

- Support the school's online safety measures.



- Engage with communications and training about online safety.
- Reinforce safe online behaviours at home.

6. Online Safety Education for Pupils

- Online safety education is integrated into the curriculum, including PSHE, computing, and bespoke interventions.
- Tailored approaches ensure pupils with SEND or complex needs receive accessible and relevant learning.
- Topics include safe technology use, recognising risks, respectful online behaviour, and reporting concerns.
- Pupils are supported to understand and manage their online presence safely.
- Pupils will be supported to develop digital resilience and self-management skills through peer education, bespoke interventions, and curriculum integration.

7. Cyberbullying and Incident Management

- Cyberbullying is addressed through education, clear reporting routes, and swift, proportionate responses.
- The school's behaviour policy guides responses to online misconduct.
- Searches and confiscations of electronic devices are conducted in line with DfE guidance and safeguarding considerations.
- AI-related risks, including misuse for bullying or misinformation, are monitored and managed.

8. Acceptable Use of Technology

- Clear agreements for pupils, staff, parents/carers, and visitors outline expectations for responsible use.
- Use of mobile devices by pupils is managed to prevent disruption and risk.
- Staff use of work devices outside school follows strict security protocols.

9. Monitoring, Reporting, and Review

- All concerns and incidents are logged on CPOMS or equivalent safeguarding systems.
- Regular monitoring of filtering and incident logs informs ongoing risk assessments.
- The policy is reviewed annually with input from governors, staff, pupils, and parents.
- The school will monitor and manage risks associated with emerging technologies, including AI tools and new digital platforms, updating policies and training accordingly.

10. Training and Support



- Induction and ongoing training for all staff on online safety risks and safeguarding.
- Specific training for DSLs and IT staff on filtering, monitoring, and incident management.
- Awareness sessions for parents/carers to support safe online behaviours at home.



Appendix 1: Pupil Acceptable Use Agreement (EYFS to KS4)

Dear Parents / Carers,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with the DSL- Molly McCann.

Please complete the signed section of this form which will be kept on record at the school. You may return the information either signed via paper methods or you can digitally sign the form and return it to school via email to the admin account.

Please select the form which you feel is most appropriate for your child.

Kind regards,

P. Tankard

Paula Tankard

Headteacher



☀ Pupils' Online Safety Rules ☀

🔒 Passwords

- Keep your passwords secret – only tell your parents/carers.
- Never use someone else's login.

💬 Be Kind Online

- Always be polite, kind, and respectful.
- Think before you type!

👉 If Something Upsets You

- Tell a teacher or parent straight away.
- Don't reply to nasty messages.

👤 Personal Information

- Don't share your name, phone number, address, or school online.
- Tell an adult if someone asks for this.

📷 Images & Videos

- Ask permission before sharing photos or videos.
- Never upload pictures of others without their permission.

🌐 Strangers Online

- Remember: not everyone online is who they say they are.
- Never agree to meet someone you only know online.

📱 Devices in School

- Phones and personal devices must be handed in at the start of the day.
- Always ask before bringing new devices.

👍 Build a Good Reputation

- Everything you do online can be traced.
- Make choices that you'll be proud of in the future.

💡 Remember: These rules are here to keep you safe now and in the future.
If you break them, teachers will look into it and may need to take action.



Online Safety Agreement

Parent name	
Parent signature	
Date	
Pupil name	
Pupil Signature	
Date	

ONLINE SAFETY AGREEMENT

Responsible Use of Equipment

- I will only use school IT equipment for activities agreed by school staff.
- In school, I will only open or delete my files when instructed by a member of staff.

Passwords and Accounts

- I will not share my passwords with anyone except my parents/carers.
- I will never use another person's username or password to pretend to be them online.

Online Behaviour

- I will ensure that all online contact is responsible, polite, and sensible.
- I will always be kind and respectful to others.

If Something Upsets Me Online

- If I see anything upsetting, unpleasant, or unsafe, I will tell my teacher or parent/carer immediately.
- If someone says or posts anything upsetting, unpleasant, or unsafe about me, I will not reply. I will tell my teacher or parent/carer straight away.

Personal Information

- I will not share personal information (such as my name, phone number, home address, interests, school, or clubs) online.
- If anyone asks me for personal information online, I will tell my teacher or parent/carer immediately.

Images and Videos

- I understand that uploading or sending my image (photographs, videos) online puts me at risk.
- I will always seek permission from my teacher or parent/carer before sharing my image.
- I will never take, share, or upload images of others without their permission. If they are a child, I will also need their parent/carer's permission.
- Even with permission, I will not upload any images, videos, sounds, or words that could upset any member of the school community now or in the future. This is cyberbullying.

Online Safety Awareness



- I understand that some people online are not who they say they are and may not be safe to contact.
- I will never arrange to meet someone I only know online. If someone asks to meet me, I will not reply and will tell a teacher or parent/carer immediately.

Online Reputation

- I understand that everything I do or receive online can be traced now and in the future.
- I know it is important to build a good online reputation.

Devices in School

- I understand that phones and other personal devices are not allowed in school.
- I will hand in any personal devices at the start of the school day.
- I will not assume that new devices can be brought into school without permission.

Age Restrictions

- I will not lie about my age to access games, apps, or social networks designed for older users, as this puts me at risk.

Consequences

- I understand that these rules are designed to keep me safe now and in the future.
- If I break these rules, my teachers will investigate and may need to take action.



Appendix 2: Staff, Governors, Volunteers Acceptable Use Agreement

When using the school's IT systems and internet, whether on site or remotely, I agree to:-

- Use technology only for professional purposes related to my role.
- Maintain confidentiality and protect sensitive information.
- Follow the school's policies on data protection, safeguarding, and online safety.
- Use strong passwords and keep them secure.
- Not access, create, or share inappropriate, offensive, or illegal material.
- Respect copyright and intellectual property rights.
- Report any online safety concerns or incidents promptly to the DSL or appropriate lead.
- Not use personal devices to take photographs or videos of pupils without permission.
- Ensure any electronic communication with pupils is professional and follows school protocols.
- Participate in required online safety and safeguarding training.
- Understand that breaches of this agreement may result in disciplinary action.

Signed:

Date:



Appendix 3: Online Safety Incident Reporting Flowchart

Step 1: Recognise Concern or Incident

- Observe or receive report of an online safety issue (e.g., cyberbullying, inappropriate content, grooming, data breach).

Step 2: Immediate Action

- Ensure pupil safety and well-being.
- If urgent, remove pupil from situation or device access.

Step 3: Report

- Report incident immediately to the Designated Safeguarding Lead (DSL) or deputy.
- Provide detailed information including time, date, involved parties, and nature of concern.

Step 4: Logging

- DSL logs the incident on CPOMS or school safeguarding system.
- Collect evidence securely without sharing beyond necessary staff.

Step 5: Investigation

- DSL, with IT and leadership support, investigates incident.
- Liaise with external agencies if required (e.g., police, social care).

Step 6: Response

- Implement appropriate interventions (disciplinary, pastoral support, education).
- Inform parents/carers as appropriate.

Step 7: Review

- Monitor outcomes and repeat risk assessments.
- Update policies or training if needed.

Step 8: Closure

- Incident closed when resolved.
- Document lessons learned and share with staff as appropriate.



Appendix 4: Filtering and Monitoring Checklist

Item	Details	Responsible Person	Review Date	Notes
Filtering Software/System	Secure filtering and monitoring systems appropriate for safeguarding pupils in special school settings will be maintained and reviewed regularly.	[IT Lead]	[Date]	Ensure updated and effective
Monitoring Software/System	Secure filtering and monitoring systems appropriate for safeguarding pupils in special school settings will be maintained and reviewed regularly.	[IT Lead]	[Date]	Regular checks for alerts
Roles Assigned for Management	[Names]	[DSL/IT Lead]	[Date]	Clear responsibilities
Review Frequency	At least annually	[DSL/IT Lead]	[Date]	Document outcomes
Incident Reporting Procedures	Established	[DSL]	[Date]	Staff aware of process
Training for Staff on Filtering & Monitoring	Completed	[DSL/Training Lead]	[Date]	Include refreshers
Access Controls	Implemented	[IT Lead]	[Date]	Password policies, permissions
Blocked Content Categories	Defined	[DSL/IT Lead]	[Date]	Align with safeguarding needs
Exceptions Process	Defined and documented	[DSL/Headteacher]	[Date]	Process for bypass requests



Appendix 5: Example Online Safety Training Log

Date	Training Topic	Staff Attendees	Trainer	Notes / Follow-up Actions
[Date]	Induction: Online Safety Overview	[Names]	[Trainer]	Completed
[Date]	Cyberbullying Awareness	[Names]	[Trainer]	Need refresher in 6 months
[Date]	Filtering and Monitoring Systems	[Names]	[IT Lead]	New software introduced
[Date]	Safeguarding and Online Safety Update	[Names]	[DSL]	Policy changes discussed
[Date]	Prevent Duty and Radicalisation	[Names]	[External Trainer]	Completed