WESTFIELD HOUSE SCHOOL

Online Safety Policy

Policy Number	EDE/POL/009	**Issue Date**	01/09/2025
Issue Number	006	**Author**	James Madine
School	Westfield House School	**Approver**	Jo Sharpe
Headteacher	Jo Murray	**Designated Safeguarding Lead**	Shona Cresey

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 2023.
- 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 (KS2 to KS4)

Key Stage 2-4 (Ages 7-16)

Pupil Agreement

- I will only use computers, gaming devices and other internet-enabled devices to access websites and services that have been agreed by the school.
- I understand that staff may check my browser history to ensure that the sites I visit are appropriate. I must not delete browser history.
- I will keep my log in details and password secret.
- I will not bring files into the school without permission or uploading material (rude, threatening, or illegal for example)
- I will not place myself/others at risk or access inappropriate (offensive/dangerous/illegal) information on the internet.
- I will not visit internet sites that have been banned by the school.
- I will only email people once the content and the person receiving the email has been approved by a staff member.
- The messages I send or the content I upload will be polite and sensible.
- I will not open an attachment or download a file, unless I have the permission of a member of staff.
- I will not give my home address, telephone number, send a photograph or video, or give any other information about me that could be used to identify me to others close to me, unless a member of staff has given permission.
- I will never arrange to meet someone I have only met on the internet and not in “real-life”.
- If I see anything I am unhappy about or get a message that I do not like, I will not reply to it and I will show a member of staff straight away.
- I will use all equipment safely and responsibly.
- I understand I must not delete others work from a computer.
- I understand that I must never use social media at school, and I should not allow others to use my device to access social media. I understand that I should tell a member of staff if a student asks me to lend them my device to access social media.
- I understand that if the above rules are not followed, I may have further restrictions placed upon my technology/internet use, supervised when using the devices or confiscated for a fixed period of time.

Parent/Carer Agreement

I agree to support the school’s rules for safe technology use and will help my child understand the importance of online safety.

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]	Ongoing	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]	Ongoing	Regular checks for alerts
Roles Assigned for Management	[Names]	[DSL/IT Lead]	Ongoing	Clear responsibilities
Review Frequency	At least annually	[DSL/IT Lead]	Ongoing	Document outcomes
Incident Reporting Procedures	Established	[DSL]	Ongoing	Staff aware of process
Training for Staff on Filtering & Monitoring	Completed	[DSL/Training Lead]	Ongoing	Include refreshers
Access Controls	Implemented	[IT Lead]	Ongoing	Password policies, permissions
Blocked Content Categories	Defined	[DSL/IT Lead]	Ongoing	Align with safeguarding needs
Exceptions Process	Defined and documented	[DSL/Headteacher]	Ongoing	Process for bypass requests

Appendix 5: 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