



E-SAFETY LOCAL PROCEDURE

Local Procedure Title	E-Safety
Home/ School/ College	Oliver House School
ACS Policy number and title	ACS 38 E-Safety
Local Procedure template reference	ACS LP 38
Local Procedure date	07/09/2026
Local Procedure review date	31/08/2027
Local Procedure Author(s)	Sarah Whatmough
Local Procedure Ratification	Checked and Approved by: Lisa Sharrock

1. Purpose

Oliver House School recognises that digital technology is an important part of learning, communication, independence and social interaction for our pupils. Many of our pupils have autism and associated needs which may increase their vulnerability online.

This procedure outlines how Oliver House School promotes online safety, protects pupils from online harm and responds to concerns or incidents involving technology, social media and internet use.

This procedure should be read alongside:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy
- Acceptable Use Agreements
- Aspris E-Safety Policy ACS38

2. Aims

Oliver House School will:

- Provide a safe online environment for all pupils.
- Teach pupils how to use technology safely and responsibly.
- Support pupils to develop age-appropriate digital literacy skills.
- Protect pupils from online abuse, exploitation, cyberbullying and harmful content.
- Promote safe use of social media, gaming platforms and communication applications.
- Ensure staff are equipped to identify and respond to online safety concerns.
- Involve parents and carers in promoting online safety.

3. Scope

This procedure applies to:

- School-owned computers, laptops, tablets and mobile devices.
- Internet access provided by the school.
- School email systems.
- Educational software and online learning platforms.
- Use of personal devices brought onto site (where permitted).
- Any online behaviour that impacts upon the safety, wellbeing or safeguarding of pupils, regardless of where the incident occurred.

4. Roles and Responsibilities

4.1 Headteacher

The Headteacher will:

- Ensure this procedure is implemented consistently.
- Ensure appropriate internet filtering and monitoring systems are operational.
- Ensure staff receive online safety training.

- Ensure online safety is embedded within the curriculum.
- Oversee responses to serious incidents.

4.2 Designated Safeguarding Lead(s) (DSL)

The DSL will:

- Lead on online safety and digital safeguarding.
- Maintain records of online safety incidents.
- Liaise with external agencies where required.
- Support investigations relating to online harm.
- Ensure concerns are managed in accordance with safeguarding procedures.

4.3 All Staff

All staff must:

- Follow school policies and acceptable use guidance.
- Supervise pupils appropriately during technology use.
- Challenge and report unsafe online behaviour.
- Record and report any safeguarding concerns immediately.
- Complete required safeguarding and online safety training.

4.4 Parents and Carers

Parents and carers are encouraged to:

- Promote safe internet use at home.
- Monitor the use of social media and online gaming where appropriate.
- Report concerns to school promptly.
- Work in partnership with school when online safety concerns arise.

5. Teaching Online Safety

Online safety education is delivered through:

- PSHE
- Computing
- Relationships and Health Education
- Themed safeguarding events and assemblies
- Individual intervention sessions where required

Teaching will be differentiated to meet pupils' communication, cognitive and social understanding needs.

Key themes include:

- Personal information and privacy
- Safe communication
- Social media awareness
- Cyberbullying
- Online relationships
- Grooming awareness
- Misinformation and scams
- Gaming safety
- Reporting concerns
- Appropriate use of artificial intelligence (AI)

6. Filtering and Monitoring

Oliver House School uses internet filtering and monitoring systems to reduce access to inappropriate or harmful content.

The school will:

- Maintain filtering systems appropriate to pupil age and vulnerability.
- Monitor internet usage where necessary to safeguard pupils.
- Review filtering arrangements regularly.

- Escalate concerns identified through monitoring systems to the DSL.
- Staff must report any weaknesses or failures in filtering immediately.

7. Mobile Phones and Personal Devices

Pupils

Use of personal devices will be managed according to individual risk assessments and school expectations.

Where permitted:

- Devices must be used responsibly.
- Internet access may be supervised.
- Staff may restrict device access if safeguarding concerns arise.

Staff

Staff must:

- Use professional judgement when using mobile devices.
- Not communicate with pupils via personal social media accounts.
- Not take photographs of pupils on personal devices.
- Adhere to the Staff Code of Conduct.

8. Cyberbullying

Cyberbullying refers to bullying through electronic means including:

- Social media
- Messaging applications
- Gaming platforms
- Online forums
- Email and text messaging

Where cyberbullying is identified:

1. Safeguarding needs will be assessed immediately.
2. Evidence will be retained where possible.
3. Parents/carers will be informed as appropriate.
4. The incident will be logged.
5. Behaviour and safeguarding procedures will be followed.
6. Support will be offered to all affected pupils.

9. Online Grooming and Exploitation

Staff must remain vigilant to indicators that a pupil may be experiencing:

- Online grooming
- Sexual exploitation
- Criminal exploitation
- Coercion or manipulation
- Online extortion or blackmail

Potential warning signs include:

- Secretive online activity
- Unexplained gifts
- Distress following internet use
- Communication with unknown individuals
- Requests to meet online contacts

Any concerns must be reported immediately to the DSL and managed through safeguarding procedures.

10. Sharing Images and Videos

Pupils will be taught:

- Not to share personal images online.
- How to seek help if asked to share images.
- How to report inappropriate requests.

If staff become aware that a pupil has shared or received inappropriate images:

- Do not forward, print or distribute images.
- Secure any device if required.
- Report immediately to the DSL.
- Follow safeguarding and child protection procedures.

Any potentially illegal content must be managed in consultation with safeguarding professionals and police where necessary.

11. Social Media

Pupils will receive support to understand:

- Safe use of social networking sites.
- Privacy settings.
- Risks of communicating with strangers.
- Managing online reputation.
- Identifying misinformation and harmful content.

Staff must not:

- Add current pupils to personal social media accounts.
- Communicate with pupils using private messaging services.
- Share confidential information online.

12. Artificial Intelligence (AI)

Oliver House School recognises emerging risks associated with AI technologies.

Staff and pupils will be educated about:

- Deepfake images and videos.
- AI-generated misinformation.
- Online scams using AI.
- Safe and ethical use of AI tools.

Any concerns involving AI-generated harmful content should be reported as safeguarding concerns.

13. Reporting Concerns

All online safety concerns must be acted upon immediately.

Internal Reporting Process

Step 1: Ensure immediate safety of the pupil.

Step 2: Inform the DSL or Deputy DSL as soon as possible.

Step 3: Record the concern on the school's electronic safeguarding system.

Step 4: Preserve evidence where appropriate.

Step 5: DSL determines next steps, including referral to:

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

Serious concerns involving exploitation, grooming, criminal activity or risk of significant harm must be escalated immediately.

14. Parents and Carers

Oliver House School will:

- Share online safety information regularly.
- Provide guidance through newsletters and workshops.
- Signpost families to online safety resources.
- Encourage open communication about online experiences.

15. Monitoring and Review

The Headteacher and DSL will review:

- Online safety incidents.
- Emerging risks and trends.
- Effectiveness of filtering and monitoring systems.
- Staff training requirements.
- Curriculum provision.

This procedure will be reviewed annually or sooner if required.