

Online Safety Policy



Approved by	<i>L. Jordan</i>
Date	Sept 2026
Review Date	Sept 2027

1. Aims

The Welbeck Federation is committed to safeguarding and promoting the welfare of all children. Technology plays an increasingly important role in children's lives both inside and outside school, and we recognise the need to educate pupils and adults to use technology safely, responsibly and positively. This policy reflects our commitment to creating a safe digital environment across all schools within the federation.

We aim to:

-  Ensure the online safety of pupils, staff, governors, volunteers and visitors.
-  Protect children from harmful or inappropriate online content, contact and conduct.
-  Empower pupils to use technology safely, respectfully and responsibly.
-  Establish clear procedures for responding to online safety concerns and incidents.
-  Meet statutory safeguarding requirements, including those relating to filtering and monitoring.
-  Promote a culture where online safety is everyone's responsibility.

The Four Areas of Online Risk

Our approach is based on the four key categories of online risk:

-  **Content:** Exposure to harmful, illegal, misleading or inappropriate content.
-  **Contact:** Harmful interactions with other users, including grooming, exploitation and online abuse.
-  **Conduct:** Unsafe or inappropriate online behaviour, including cyberbullying and sharing harmful content.
-  **Commerce:** Online scams, gambling, phishing, fraud and financial exploitation.

2. Legislation and Guidance

This policy should be read alongside:

-  Keeping Children Safe in Education (KCSIE)
-  Teaching Online Safety in Schools
-  Relationships Education, Relationships and Sex Education (RSE) and Health Education

-  Searching, Screening and Confiscation
-  Prevent Duty Guidance
-  The Education Act 2011
-  The Children Act 1989 and 2004
-  UK General Data Protection Regulation (UK GDPR)
-  Data Protection Act 2018
-  Equality Act 2010

This policy is also supported by guidance from the UK Safer Internet Centre and Education for a Connected World Framework.

3. Roles and Responsibilities

Governing Body

Governors are responsible for:

-  Monitoring the effectiveness of this policy.
-  Ensuring appropriate filtering and monitoring systems are in place.
-  Receiving regular safeguarding reports that include online safety matters.
-  Ensuring staff receive appropriate online safety training.
-  Ensuring pupils are taught how to stay safe online.

Executive Headteacher

Lisa Jordan has overall responsibility for ensuring this policy is implemented consistently across the federation.

The Executive Headteacher will:

-  Ensure robust online safety procedures are in place.
-  Support staff in implementing this policy.
-  Ensure online safety remains a key safeguarding priority.
-  Report significant concerns to governors as appropriate.

Safeguarding Team

The Safeguarding team takes lead responsibility for online safeguarding.

Safeguarding Team	
Designated Safeguarding Lead	Deputy Safeguarding Leads
 Lisa Jordan	 Matt Walker  Joanne Turner  Caroline Goodall

Responsibilities include:

-  Managing online safety concerns and incidents.
-  Recording concerns through CPOMS.
-  Liaising with external agencies where necessary.
-  Supporting staff and families.
-  Reviewing trends and emerging risks.
-  Receiving and acting upon filtering and monitoring alerts.

Computing Lead

Laura Patrick will:

-  Support online safety curriculum development.
-  Ensure online safety education is progressive and age appropriate.
-  Monitor the effectiveness of online safety teaching.

IT Provider

Atom IT is responsible for:

-  Maintaining secure technical systems.
-  Providing filtering and monitoring solutions.
-  Network security and cyber-security measures.
-  Responding to technical incidents and vulnerabilities.
-  Supporting the federation in meeting DfE filtering and monitoring expectations.

Staff

All staff must:

-  Read and follow this policy.
-  Complete annual safeguarding and online safety training.
-  Report concerns promptly.

- 🌐 Model safe and professional use of technology.
- 🌐 Maintain professional boundaries online.
- 🌐 Support pupils to use technology safely.

Parents/Carers

Parents/carers are expected to:

- 🌐 Notify a member of staff or the Executive Headteacher of any concerns or queries regarding this policy
- 🌐 Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

[What are the issues? - UK Safer Internet Centre](#)

[Help & advice | Childnet](#)

[Parents and Carers resource sheet | Childnet](#)

4. Filtering and Monitoring

The Welbeck Federation uses Atom IT to provide filtering and monitoring services across federation networks and devices.

The Federation ensures:

- 🌐 Internet access is filtered appropriately.
- 🌐 Harmful and inappropriate content is blocked.
- 🌐 Monitoring systems identify potentially concerning activity.
- 🌐 Safeguarding alerts are reviewed by designated safeguarding staff.
- 🌐 Filtering and monitoring arrangements are reviewed at least annually.
- 🌐 Systems comply with current DfE filtering and monitoring standards.

Where staff require access to blocked content for educational purposes, requests must be authorised through the agreed procedure.

5. Educating Pupils About Online Safety

Online safety is embedded throughout the curriculum and taught through:

- 🌐 Computing
- 🌐 PSHE
- 🌐 Relationships Education
- 🌐 Assemblies
- 🌐 Safeguarding events
- 🌐 Safer Internet Day activities

Pupils will learn about:

- 🌐 Protecting personal information.
- 🌐 Secure passwords.
- 🌐 Online relationships.
- 🌐 Cyberbullying.
- 🌐 Misinformation and disinformation.
- 🌐 Online scams and fraud.
- 🌐 Social media.
- 🌐 Gaming and livestreaming.
- 🌐 Online reputation.
- 🌐 Consent and image sharing.
- 🌐 Healthy screen use.
- 🌐 Artificial intelligence and emerging technologies.
- 🌐 How and when to seek help.

Teaching will be adapted where necessary for vulnerable pupils and those with SEND.

6. Artificial Intelligence (AI)

The Federation recognises the growing role of Artificial Intelligence (AI) technologies.

Pupils will be taught:

- 🌐 How AI tools work.
- 🌐 The benefits and limitations of AI.
- 🌐 The importance of checking information generated by AI.

- 🌐 How to use AI responsibly and ethically.

Staff must:

- 🌐 Use only approved AI tools.
- 🌐 Never enter confidential or personal information into public AI systems.
- 🌐 Check AI-generated content for accuracy, bias and suitability before use.

AI should support professional judgement and never replace safeguarding responsibilities.

7. Educating Parents and Carers

The Federation will support parents and carers through:

- 🌐 Newsletters.
- 🌐 Website resources.
- 🌐 Information events.
- 🌐 Parent communications.
- 🌐 Signposting to trusted online safety organisations.

Parents are encouraged to:

- 🌐 Monitor their child's online activity.
- 🌐 Discuss online safety regularly.
- 🌐 Report concerns to the school promptly.
- 🌐 Support the school's expectations regarding technology use.

8. Cyberbullying

Cyberbullying is bullying that takes place through digital technologies such as:

- 🌐 Social media
- 🌐 Messaging apps
- 🌐 Online gaming platforms
- 🌐 Emails
- 🌐 Text messages

The Federation takes all reports of cyberbullying seriously.

Where incidents occur, we will:

-  Investigate promptly.
-  Support victims.
-  Educate pupils involved.
-  Apply sanctions where appropriate.
-  Involve parents where necessary.
-  Refer safeguarding concerns to the DSL team.

9. Mobile Phones and Personal Devices

Pupils may bring a mobile phone to school only with parental agreement (see Mobile Phone Policy).

Where mobile phones are brought to school:

-  Phones must be handed into the school office at the start of the day.
-  Phones are stored securely.
-  Phones must not be used during the school day.
-  Misuse may result in confiscation and additional sanctions.

Personal devices should not be used by pupils to photograph, record or communicate during the school day unless authorised by staff.

10. Staff Use of Technology

Staff are expected to:

-  Use Federation systems professionally.
-  Keep passwords secure.
-  Use only authorised software and services.
-  Follow GDPR and data protection requirements.
-  Use official communication systems only.
-  Maintain professional boundaries online.

Staff must not:

-  Communicate with pupils through personal social media accounts.
-  Share confidential information.
-  Access inappropriate material.
-  Use personal devices in ways that compromise safeguarding or professional standards.

11. Responding to Online Safety Concerns

Any member of staff who becomes aware of an online safety concern must:

1. Reassure and listen to the child.
2. Avoid investigating independently.
3. Record the concern.
4. Report immediately to a DSL.

Where necessary, concerns may be referred to:

-  Children's Social Care
-  Police
-  CEOP
-  Local Authority Designated Officer (LADO)
-  Other relevant safeguarding agencies

Online safety incidents will be recorded through CPOMS and monitored for trends.

12. Cyber Security

The Federation takes cyber security seriously.

Measures include:

-  Secure password protocols.
-  Multi-factor authentication where appropriate.
-  Regular software updates.
-  Antivirus and malware protection.
-  Network monitoring.

-  Staff cyber-security awareness training.
-  Phishing awareness training.
-  Secure data storage and transfer procedures.

Any suspected cyber-security incident must be reported immediately.

13. Training

All staff receive:

-  Online safety training during induction.
-  Annual safeguarding updates.
-  Relevant online safety updates throughout the year.
-  Training on filtering and monitoring responsibilities.

Governors also receive appropriate safeguarding and online safety training.

14. Monitoring and Review

The Federation will:

-  Monitor online safety incidents and trends.
-  Review filtering and monitoring arrangements annually.
-  Evaluate curriculum effectiveness.
-  Review this policy annually or sooner if required by legislative or safeguarding updates.

The policy will be submitted to governors for approval and review annually.

15. Related Policies

-  This policy should be read alongside:
-  Child Protection Policy
-  Behaviour Policy
-  Staff Code of Conduct
-  Data Protection Policy

-  Mobile Phone Policy
-  Relationships and Health Education Policy
-  Acceptable Use Policy & Agreement
-  Remote Learning Policy
-  Complaints Policy