

BOLD FUTURES



Bold Futures Federation
Online Safety Policy

Document Name: Online Safety Policy

Document ID: N/A

Current Version: 3.0

Status: Approved

Signed *L.Coombs, L.manser*
Print Name: L.Coombs, L.Manser

Signed: Robyn Jarret (Governor Approval)
Print Name: Robyn Jarret

BOLD FUTURES



POLICY CHANGE HISTORY

Version	Date	Status	Policy Owner	Governor Approval	Comment
1.0	November 2021		L.Coombs		
2.0	November 2023		L.Coombs		Update of roles and responsibilities Additional information added about filtering and monitoring Flow chart added to explain process of misconduct
2.1	October 2024		L.Coombs		No changes required
2.2	October 2025		L.Coombs		Update to be across federation document
3.0	August 2026		L.Coombs and L. Manser		Renamed Online Safety Policy and comprehensively reviewed to reflect current safeguarding, filtering and monitoring, cyber-security, AI and digital technology expectations

1. Purpose

Bold Futures Federation is committed to safeguarding and promoting the welfare of children both online and offline.

Digital technology provides significant opportunities for teaching, learning, communication, creativity and participation in the wider world. However, its use can also expose children and adults to risks.

Online safety is therefore an integral part of the Federation's safeguarding responsibilities and is not treated solely as a Computing or technical matter.

This policy sets out how Bold Futures Federation will:

- protect children and other members of the Federation community from online harm;
 - provide a safe digital environment for teaching and learning;
 - ensure appropriate filtering and monitoring arrangements are in place;
 - educate pupils to become safe, responsible, respectful and critical users of technology;
 - ensure staff understand and fulfil their online-safety responsibilities;
 - support parents and carers in understanding online risks;
 - respond appropriately to online-safety incidents and concerns;
 - manage risks associated with emerging technologies, including artificial intelligence;
 - maintain appropriate links between safeguarding, curriculum and technical security; and
 - ensure arrangements are regularly reviewed as technology, patterns of use and risks change.
-

2. Scope

This policy applies across all schools within Bold Futures Federation.

It applies to:

- pupils;
- teaching and support staff;
- senior leaders;
- governors;
- volunteers;
- trainees;
- supply and agency staff;
- contractors;
- visitors;
- parents and carers where relevant; and

- any other users of Federation digital systems.

It applies to:

- Federation devices;
- networks and internet connections;
- cloud-based services;
- email and communication systems;
- websites and online platforms;
- management and safeguarding systems;
- cameras and recording equipment;
- artificial intelligence tools;
- video-conferencing and remote-learning platforms;
- personal devices where their use affects the school or its pupils; and
- online behaviour outside school where there is a safeguarding concern or a clear connection with the school community.

3. Relationship with Safeguarding

Online safety is a safeguarding responsibility.

The Designated Safeguarding Lead (DSL) holds lead responsibility for online safety as part of their safeguarding role.

Any online concern that indicates that a child may be at risk of harm must be dealt with in accordance with the Federation's Child Protection and Safeguarding Policy.

This includes concerns relating to:

- abuse;
- exploitation;
- grooming;
- child-on-child abuse;
- sexual harassment;
- sharing of nude or semi-nude images;
- radicalisation and extremism;
- self-harm or suicide;
- coercion or threats;
- criminal or financial exploitation;
- online bullying;
- harmful or inappropriate contact; and
- any other online behaviour which may place a child at risk.

Staff must not investigate safeguarding concerns themselves. Concerns must be reported immediately to the DSL or a deputy DSL through the Federation's safeguarding procedures.

Where the concern relates to the conduct of an adult working with children, the Federation's safeguarding procedures for allegations and low-level concerns must be followed.

4. Related Policies

This policy should be read alongside the Federation's:

- **Child Protection and Safeguarding Policy;**
- **Acceptable Use of IT and Digital Technology Policy – Staff, Governors and Other Adults;**
- **Data Protection Policy;**
- **Computing Policy;**
- **Social Media Policy;**
- **Remote Education Policy;**
- **Behaviour Policy;**
- **Anti-Bullying Policy;**
- **Staff Code of Conduct;**
- **Whistleblowing Policy;** and
- relevant photography, video and image-sharing guidance.

Where an online incident is a safeguarding concern, the Child Protection and Safeguarding Policy takes precedence.

The Acceptable Use Policy sets out the expectations placed on adults using Federation technology.

Detailed expectations regarding staff and governor social-media use are contained within the Social Media Policy.

Detailed curriculum provision is contained within the Computing Policy.

5. Statutory and National Guidance

This policy has regard to relevant legislation and guidance, including:

- Keeping Children Safe in Education 2026;
- Department for Education guidance on Meeting Digital and Technology Standards in Schools and Colleges, including the Filtering and Monitoring Core Standard and Cyber Security Core Standard;
- the Education for a Connected World framework;
- Department for Education guidance concerning generative artificial intelligence in education;
- the Generative AI: Product Safety Standards;

- the Online Safety Act 2023;
- the Data Protection Act 2018 and UK GDPR as amended;
- the Data (Use and Access) Act 2025;
- the Prevent Duty;
- relevant UK Council for Internet Safety guidance;
- UK Safer Internet Centre guidance; and
- relevant local safeguarding-partnership procedures.

The Federation will update its approach when statutory requirements or national guidance change.

6. Understanding Online Risk

Keeping Children Safe in Education identifies four broad areas of online-safety risk.

6.1 Content

Being exposed to illegal, inappropriate or harmful material.

Examples may include:

- pornography;
- sexual content;
- racism and discriminatory content;
- misogyny;
- hate speech;
- violent content;
- self-harm and suicide content;
- eating-disorder content;
- misinformation and disinformation;
- manipulated or AI-generated material;
- radicalising or extremist material; and
- content that is inappropriate for a child's age or development.

6.2 Contact

Being subjected to harmful interaction with other users.

Examples may include:

- adults posing as children;
- grooming;
- sexual exploitation;
- criminal exploitation;
- financial exploitation;
- coercion;

- inappropriate requests for images or information;
- harmful communication from strangers;
- peer pressure; and
- inappropriate commercial contact.

6.3 Conduct

Online behaviour that increases the likelihood of, or causes, harm.

Examples may include:

- online bullying;
- abusive or threatening communication;
- sexual harassment;
- sharing nude or semi-nude images;
- sharing another person's information or images without permission;
- discriminatory behaviour;
- impersonation;
- harmful online challenges;
- deliberately spreading false information; and
- inappropriate use of artificial intelligence or digital content.

6.4 Commerce

Risks associated with online financial and commercial activity.

Examples may include:

- online gambling;
- gaming-related purchases;
- inappropriate advertising;
- scams;
- phishing;
- fraudulent websites;
- financial exploitation;
- in-app purchases; and
- pressure to spend money online.

The Federation recognises that these areas frequently overlap.

7. Emerging and Evolving Risks

The Federation recognises that online risks change rapidly.

Online-safety provision will therefore consider emerging technologies and behaviours including:

- generative artificial intelligence;
- AI companions and chatbots;
- deepfakes and synthetic media;
- misinformation and disinformation;
- image manipulation;
- immersive and virtual environments;
- livestreaming;
- online gaming and in-game communication;
- social-media trends and challenges;
- encrypted and disappearing-message services;
- location sharing;
- algorithms and recommendation systems; and
- new platforms or devices used by children.

The Federation will not rely solely upon naming individual applications or websites. Pupils will instead be taught transferable knowledge and strategies that can be applied to unfamiliar technologies.

8. Roles and Responsibilities

Online safety is a shared responsibility, but clear leadership and accountability are essential.

8.1 Governing Body

The Governing Body is responsible for ensuring that the Federation has appropriate arrangements to safeguard children online.

Governors will:

- approve this policy and associated policies and review their effectiveness;
- ensure appropriate filtering and monitoring systems are in place;
- ensure filtering and monitoring arrangements are reviewed at least annually and that these reviews are recorded;
- receive appropriate information about online-safety incidents and trends;
- ensure safeguarding and technical responsibilities are clearly assigned;
- receive appropriate safeguarding, online-safety and cyber-security training;
- provide strategic challenge and oversight;
- ensure staff understand their responsibilities regarding filtering and monitoring;
- consider online safety as part of wider safeguarding oversight; and
- monitor pupils' knowledge of online safety.

A named Safeguarding Governor will take a particular interest in online safety.

The Safeguarding Governor will meet appropriately with the DSL and, where relevant, the Computing Lead and will receive anonymised information relating to:

- significant online-safety concerns;
 - patterns or trends;
 - filtering and monitoring;
 - curriculum provision;
 - staff training; and
 - actions taken to reduce identified risks.
-

8.2 Executive Headteacher/Headteachers and Senior Leaders

Senior leaders have a duty of care for the safety of all members of the school community.

They will:

- establish a culture in which online safety is understood as part of safeguarding;
 - ensure that appropriate policies, systems and procedures are in place;
 - ensure that roles and responsibilities are clearly defined;
 - support the DSL in fulfilling their online-safety responsibilities;
 - ensure appropriate staff training takes place;
 - ensure staff understand the filtering and monitoring arrangements;
 - ensure suitable technical support is available;
 - work with the DSL, Computing Lead, Safeguarding Governor and IT provider to review filtering and monitoring;
 - ensure concerns identified through filtering and monitoring are acted upon;
 - ensure appropriate arrangements exist for serious incidents or allegations involving staff; and
 - ensure learning from incidents informs future practice.
-

8.3 Designated Safeguarding Lead

The DSL holds lead responsibility for online safety within their safeguarding role.

The DSL will:

- maintain an up-to-date understanding of online-safety risks;
- receive appropriate and regularly updated online-safety training;
- understand the filtering and monitoring arrangements in place;
- act upon relevant safeguarding alerts;
- ensure online-safety incidents involving safeguarding are recorded appropriately;
- identify patterns and trends;
- liaise with the Computing Lead, IT provider and senior leaders;
- make or support referrals to external agencies where required;
- ensure safeguarding procedures are followed following an online incident;

- contribute to filtering and monitoring reviews;
- ensure vulnerable pupils or groups are considered when assessing online risks; and
- report appropriate information to senior leaders and governors.

The DSL's safeguarding responsibility cannot be delegated to the Computing Lead or IT provider.

8.4 Computing Lead

The Computing Lead supports the DSL but has a different primary responsibility.

The Computing Lead will:

- lead the development and review of online-safety education;
- ensure the online-safety curriculum is progressive from EYFS to Year 6;
- ensure provision reflects the Education for a Connected World framework;
- map online-safety learning through Computing and the wider curriculum (particularly PSHE and Healthy Relationships);
- monitor implementation and impact;
- support staff with curriculum knowledge;
- identify appropriate resources and professional development;
- provide age-appropriate updates relating to emerging technologies and risks;
- support the DSL and IT provider with the review of filtering and monitoring;
- promote appropriate national initiatives such as Safer Internet Day;
- support communication with parents and carers; and
- ensure curriculum learning reflects patterns of concern identified through safeguarding and monitoring.

The Computing Lead does not replace the DSL's safeguarding responsibility.

8.5 Teaching and Support Staff

All staff must understand that online safety is part of safeguarding.

Staff are responsible for:

- reading and following this policy;
- following the Child Protection and Safeguarding Policy;
- following the Federation's Acceptable Use Policy;
- maintaining awareness of relevant online risks;
- completing required online-safety training;
- understanding the filtering and monitoring systems used by the school at a level appropriate to their role;
- knowing how to report concerns about filtering or monitoring;

- reporting safeguarding concerns immediately;
- modelling safe, responsible and professional use of technology;
- supervising pupils' use of technology appropriately;
- reinforcing online-safety messages throughout the curriculum;
- using only Federation-approved methods to communicate with pupils;
- selecting appropriate digital content and resources;
- being alert to signs that a pupil may be experiencing online harm; and
- maintaining professional boundaries online.

Staff must never assume that filtering systems remove the need for appropriate adult supervision.

8.6 IT Support Provider

The IT provider has technical responsibility for implementing and maintaining agreed technical controls.

The provider will work with Federation leaders to ensure:

- technical infrastructure is appropriately secure;
- filtering systems are configured appropriately;
- monitoring arrangements operate as agreed;
- systems are maintained and updated;
- access controls are appropriate;
- relevant security updates and patches are applied;
- technical concerns are escalated promptly;
- filtering and monitoring reports are available to relevant school staff;
- appropriate backup and recovery arrangements are maintained; and
- the Federation is supported in meeting current DfE digital and technology standards.

The Federation retains overall responsibility for safeguarding and cannot outsource this responsibility to its IT provider.

8.7 Pupils

Pupils will be taught to:

- use Federation technology responsibly;
- follow pupil acceptable-use expectations;
- keep personal information safe;
- protect passwords and accounts;
- communicate respectfully;
- recognise inappropriate or harmful behaviour;
- recognise unreliable, misleading or manipulated content;

- recognise online scams and suspicious communications;
- understand that online actions can have consequences;
- seek help when something makes them worried or uncomfortable;
- report concerning content or behaviour to a trusted adult;
- understand that reporting a concern is the right thing to do;
- understand how technology can affect health and wellbeing;
- use age-appropriate services; and
- increasingly make informed and responsible decisions as they become more independent.

Pupils should understand that school monitoring systems exist to help keep users safe.

8.8 Parents and Carers

The Federation recognises parents and carers as important partners in online safety.

The Federation will support families through:

- school websites;
- newsletters;
- workshops or information sessions;
- parent events;
- guidance following emerging concerns;
- Safer Internet Day and similar initiatives;
- signposting to appropriate external support; and
- communication about significant changes in online risks where appropriate.

Parents and carers will be encouraged to:

- reinforce online-safety messages at home;
 - discuss online activity openly with their children;
 - use age-appropriate parental controls;
 - consider age restrictions;
 - monitor their child's use of technology appropriately;
 - seek advice when required; and
 - report relevant concerns to the school.
-

9. Filtering and Monitoring

Filtering and monitoring are an important part of the Federation's safeguarding arrangements.

However, no technical system can eliminate all online risk. Filtering and monitoring must operate alongside:

- effective safeguarding practice;
- pupil education;
- staff awareness;
- adult supervision;
- appropriate behaviour expectations; and
- effective reporting systems.

9.1 Governance and Responsibility

Filtering and monitoring arrangements will be agreed and reviewed by appropriate senior leaders working with:

- the DSL;
- the Computing Lead;
- the IT provider; and
- the responsible governor.

The DSL has lead safeguarding responsibility.

The IT provider has responsibility for technical implementation and support.

Senior leaders retain overall responsibility for ensuring arrangements are appropriate and effective.

10. Filtering

The Federation will maintain appropriate filtering systems to restrict access to illegal, inappropriate and harmful content.

Filtering will:

- operate on the Federation's internet-connected systems and devices as appropriate;
- reflect the age and needs of users;
- differentiate access where appropriate between staff and pupils;
- restrict access to illegal content;
- limit access to harmful and inappropriate content;
- be capable of being reviewed and adapted as risks change;
- support educational use without imposing unreasonable restrictions on learning;
- be regularly checked to ensure it is operating as intended; and
- provide appropriate information to enable concerns and breaches to be investigated.

The Federation will ensure that recognised lists relating to illegal content are appropriately incorporated through its filtering provider.

Filtering must not be disabled or circumvented by users.

Where staff believe legitimate educational content has been incorrectly filtered, they should use the agreed procedure to request review rather than attempting to bypass the system.

Where harmful material is accessed despite filtering, this must be reported appropriately.

11. Monitoring

The Federation will use proportionate monitoring arrangements to help identify online-safety and safeguarding concerns.

Monitoring will include:

- technical monitoring of network and internet activity;
- review of filtering logs;
- automated alerts;
- monitoring provided through a third-party service (IT and internet provider, Harrap);
- review of activity on Federation-owned devices;
- appropriate physical supervision by adults; and
- other proportionate arrangements informed by safeguarding risk.

Relevant alerts will be reviewed by appropriately trained staff.

Safeguarding alerts must be escalated promptly to the DSL or a deputy DSL.

The Federation will ensure that:

- monitoring responsibilities are clearly allocated;
- staff understand how concerns are escalated;
- alerts are acted upon within an appropriate timeframe;
- actions and outcomes are recorded where relevant;
- monitoring arrangements reflect pupil age and vulnerability;
- arrangements comply with relevant data-protection requirements; and
- monitoring information is used to identify trends and improve provision.

Users will be informed that Federation systems and devices may be monitored.

12. Review of Filtering and Monitoring

The Federation will conduct a formal review of filtering and monitoring provision at least once every academic year.

The review will involve appropriate representatives including:

- senior leaders;
- the DSL;
- the IT provider;
- the Computing Lead where appropriate; and
- the responsible governor.

The review will consider:

- whether filtering is working as intended;
- whether monitoring arrangements are effective;
- whether filtering applies appropriately across relevant internet-connected devices and locations;
- the age and needs of pupils;
- pupils who may be at increased risk;
- patterns of incidents and attempted access;
- emerging technologies and risks;
- staff understanding of arrangements;
- whether concerns are escalated effectively; and
- whether existing arrangements remain proportionate and appropriate.

A record of the review and actions arising from it will be maintained.

In addition to the annual formal review, operational checks will take place during the year, including appropriate filtering tests and review of relevant logs and alerts.

Significant safeguarding incidents, major technological changes or changes to provision may trigger an additional review.

13. Artificial Intelligence

Artificial intelligence is an increasingly significant part of children's digital lives.

Online-safety education will therefore include age-appropriate understanding of AI.

Pupils will progressively learn that:

- AI-generated information may be incorrect or fabricated;
- AI may reflect bias contained within data or design;
- images, audio and video may be artificially generated or manipulated;
- people may use AI to mislead, scam, impersonate or cause harm;
- personal information should not be shared unnecessarily with AI systems;
- AI responses should be critically evaluated;

- AI is a tool rather than an unquestionable source of authority; and
- concerns about AI-generated content should be reported to a trusted adult.

Learner-facing AI

Where a generative AI product is considered for direct pupil use, the Federation will assess its suitability before use.

Consideration will include:

- intended age range;
- educational purpose;
- safeguarding;
- filtering and content moderation;
- monitoring and reporting;
- privacy and data protection;
- security;
- SEND and accessibility;
- potential for inappropriate interaction;
- impact on children's cognitive, emotional and social development; and
- supplier information regarding product safety.

Pupil use of generative AI will only take place where the Federation considers it appropriate, safe and educationally justified.

Staff use of AI is governed principally through the Acceptable Use of IT and Digital Technology Policy and Data Protection Policy.

14. Online Safety Curriculum

Online safety will be taught progressively from EYFS to Year 6.

It is:

- a discrete and planned component of the Computing curriculum;
- reinforced through other curriculum subjects;
- supported through assemblies and pastoral provision;
- revisited in response to emerging risks and incidents; and
- reinforced through wider safeguarding practice.

The curriculum will be informed by the UK Council for Internet Safety Education for a Connected World framework.

Learning will include age-appropriate teaching about:

- self-image and identity;

- online relationships;
- online reputation;
- online bullying;
- managing online information;
- health, wellbeing and lifestyle;
- privacy and security;
- copyright and ownership;
- misinformation and disinformation;
- artificial intelligence;
- phishing and scams;
- reporting concerns; and
- respectful and responsible online behaviour.

Teaching will focus on developing knowledge, judgement and resilience rather than relying solely upon lists of prohibited applications or activities.

15. Safe Use of Digital Resources

Teachers must make reasonable checks that planned digital resources are appropriate for pupils.

When pupils access the internet:

- use should have a clear educational purpose;
- pupils should be appropriately supervised;
- age-appropriate resources should be selected;
- staff should remain alert to unexpected content;
- pupils should know how to report inappropriate content; and
- safeguarding procedures should be followed where a concern arises.

Search engines and other online services should be used in an age-appropriate manner.

Staff should not rely solely upon a resource being labelled "educational" when deciding whether it is suitable.

16. Social Media and Online Communication

Detailed expectations regarding staff and governor use of social media are set out within the Federation's Social Media Policy.

Key safeguarding principles include:

- staff must maintain professional boundaries online;
- personal social-media accounts must not be used to communicate with current pupils;
- staff must not accept pupils as personal social-media contacts;
- Federation information must not be published through unauthorised accounts;
- confidential or personal information must not be disclosed;
- inappropriate online contact involving a pupil must be reported; and
- official Federation social-media activity must be appropriately authorised.

Pupils will be taught about age restrictions, privacy, online reputation and safe communication as part of the online-safety curriculum.

17. Images, Video and Livestreaming

Images, recordings and livestreamed activity involving pupils must be managed in accordance with safeguarding and data-protection requirements.

The Federation will ensure appropriate consideration is given to:

- purpose;
- safeguarding;
- privacy;
- parental information and consent where applicable;
- access;
- storage;
- publication;
- retention; and
- deletion.

Staff must follow Federation guidance concerning photography and video.

Personal devices must not be used to photograph or record pupils except where explicitly authorised under Federation procedures.

Further requirements are contained within the Data Protection Policy, Acceptable Use Policy and relevant image-sharing guidance.

18. Video Conferencing and Remote Education

Where video conferencing or remote education is used:

- Federation-approved platforms must be used;

- professional boundaries must be maintained;
- appropriate accounts must be used;
- staff must consider their background and surroundings;
- confidential information must not inadvertently be displayed;
- safeguarding procedures apply in the same way as during face-to-face provision;
- inappropriate behaviour or content must be reported;
- pupils must be given age-appropriate expectations for use; and
- data protection and security requirements must be followed.

Further arrangements are detailed in the Remote Education Policy and Acceptable Use of IT and Digital Technology Policy.

19. Personal and Portable Devices

Use of mobile phones, smart watches, tablets and other personal devices must be consistent with Federation policies.

Staff personal-device use is governed by the Acceptable Use of IT and Digital Technology Policy, Staff Code of Conduct and Mobile Phone Policy.

Pupil use of personal devices will be governed by individual school arrangements and relevant behaviour and safeguarding procedures.

Personal mobile-data connections must not be used as a means of deliberately bypassing Federation safeguarding controls.

Where new types of connected devices are proposed for educational use, consideration will be given to their:

- educational benefit;
 - safeguarding implications;
 - data security;
 - privacy;
 - connectivity; and
 - ability to capture or share information.
-

20. Online Bullying and Child-on-Child Abuse

Online bullying and online child-on-child abuse will be taken seriously.

Online behaviour may form part of a wider safeguarding concern and should not automatically be treated as a behaviour issue only.

Concerns may include:

- repeated abusive messaging;
- exclusion or humiliation online;
- spreading rumours;
- discriminatory abuse;
- sexual harassment;
- non-consensual sharing of images;
- threats;
- impersonation;
- coercion;
- harmful group-chat behaviour; and
- the use of edited or AI-generated content to target another person.

Staff must follow the Federation's Child Protection and Safeguarding Policy, Behaviour Policy and Anti-Bullying Policy as appropriate.

21. Sharing Nude and Semi-Nude Images

Where staff become aware of the sharing of nude or semi-nude images involving children, the concern must be reported immediately to the DSL.

Staff must:

- not view imagery unless there is a clear and necessary safeguarding reason and the DSL determines this is appropriate;
- not copy, print, save or forward imagery;
- not ask pupils to send imagery;
- not delete relevant information unless directed to do so through appropriate safeguarding procedures;
- not conduct their own investigation; and
- follow current UKCIS and safeguarding guidance.

Where there is any concern that imagery may constitute illegal content, specialist advice will be sought through appropriate safeguarding and law-enforcement routes.

22. Radicalisation and Extremism

Online content and communication can play a role in radicalisation.

Staff must remain alert to online behaviour that may indicate vulnerability to extremist influence.

Relevant concerns must be reported to the DSL and dealt with in accordance with the Child Protection and Safeguarding Policy and the Federation's Prevent procedures.

Filtering forms one element of this protection but does not replace staff vigilance or safeguarding education.

23. Online Safety and Vulnerable Pupils

The Federation recognises that some pupils may be more vulnerable to online harm.

This may include, but is not limited to:

- pupils with SEND;
- pupils with communication difficulties;
- pupils experiencing social or emotional difficulties;
- children in care or previously in care;
- pupils experiencing abuse or exploitation;
- pupils with limited understanding of risk;
- pupils experiencing isolation; and
- pupils whose circumstances increase vulnerability.

Provision, teaching, filtering, monitoring and support will take account of individual needs where appropriate.

The Federation will avoid assuming that all pupils of the same age have the same level of online understanding or vulnerability.

24. Reporting Online Safety Concerns

All members of the school community should know how to report an online-safety concern.

A concern involving the safety or welfare of a child

Report immediately to the DSL or a deputy DSL in accordance with the Child Protection and Safeguarding Policy.

Concern regarding filtering or monitoring

Report through the Federation's agreed route to the appropriate DSL, senior leader, Computing Lead and/or IT provider according to the nature of the concern.

Cyber-security concern

Follow the Federation's cyber-security and Acceptable Use procedures.

Data-protection concern

Follow the Federation's Data Protection Policy and data-breach procedure.

Concern about an adult

Follow Federation procedures for allegations, low-level concerns or whistleblowing.

Immediate risk or suspected criminal activity

The DSL or senior leader will seek advice from or make referrals to relevant agencies, including the police, children's social care or other safeguarding services where appropriate.

25. Responding to Online Safety Incidents

The Federation's response will depend upon the nature of the concern.

When an incident is reported:

1. **Safeguarding comes first.**
 2. The immediate welfare of any child involved will be considered.
 3. The DSL will be informed where there is a safeguarding concern.
 4. Relevant information will be recorded.
 5. Evidence will be preserved where appropriate without unnecessarily viewing, copying or distributing harmful material.
 6. Staff will not conduct an inappropriate independent investigation.
 7. Advice or referral will be sought from relevant agencies where necessary.
 8. Parents or carers will normally be informed where appropriate, unless doing so could place a child at greater risk or conflict with safeguarding advice.
 9. Appropriate support will be provided to those affected.
 10. Relevant behaviour, disciplinary, safeguarding, data-protection or cyber-security procedures will be followed.
 11. Learning from significant incidents will inform future safeguarding, filtering, monitoring, curriculum or staff-training arrangements.
-

26. Illegal or Suspected Illegal Content

Where illegal online material or activity is suspected:

- the concern must be reported immediately;
- the DSL and appropriate senior leader should be informed;
- users must not deliberately continue accessing the content;
- content must not be forwarded or distributed;
- staff must not undertake their own investigation;
- evidence should be preserved in accordance with safeguarding and law-enforcement advice; and
- police or other agencies will be contacted where appropriate.

Particular care must be taken where an incident may involve child sexual abuse material.

Staff must not print, save, copy, forward or unnecessarily view such imagery.

27. Record Keeping and Learning from Incidents

Relevant online-safety incidents will be recorded through appropriate safeguarding or operational systems.

Records may be used to identify:

- recurring concerns;
- vulnerable individuals or groups;
- curriculum needs;
- staff-training needs;
- weaknesses in filtering or monitoring;
- emerging online trends; and
- changes required to policy or practice.

Information provided to governors will be anonymised as appropriate.

28. Staff Training

All staff will receive appropriate online-safety information and training as part of safeguarding provision.

This will include:

- online safety as a safeguarding responsibility;
- current and emerging risks;
- the four areas of online risk;
- filtering and monitoring;
- how to report concerns;
- pupil vulnerability;
- professional boundaries;
- cyber security;
- data protection;
- artificial intelligence;
- harmful online content and communication; and
- relevant updates arising from incidents or changes in guidance.

Staff with specific responsibilities will receive additional role-appropriate training.

29. Pupil Voice

The Federation will use pupil voice where appropriate to understand:

- how pupils use technology;
- online platforms and trends relevant to them;
- whether pupils know how to report concerns;
- their understanding of online risks;
- how safe they feel online;
- curriculum impact; and
- areas where further teaching or support may be required.

Pupil voice will be used alongside safeguarding information and professional judgement and will not replace risk assessment.

30. Monitoring and Evaluation of the Policy

The effectiveness of online-safety provision will be monitored through a combination of:

- safeguarding information;
- filtering and monitoring reviews;
- incident analysis;
- curriculum monitoring;
- pupil voice;
- staff voice;
- parent feedback;
- lesson and work scrutiny where appropriate;

- Computing subject monitoring;
- governor oversight; and
- technical review.

Findings will inform:

- curriculum development;
- safeguarding practice;
- staff training;
- parent communication;
- technical controls;
- school improvement; and
- future policy review.

31. Policy Review

This policy will be formally reviewed at least annually.

It will also be reviewed sooner where required because of:

- changes to statutory guidance;
- changes to DfE digital and technology standards;
- changes to legislation;
- significant online-safety incidents;
- changes to filtering or monitoring systems;
- new technologies;
- emerging risks;
- changes to Federation infrastructure; or
- learning arising from safeguarding reviews.

The Governing Body will approve the policy.

Appendix 1 – Online Safety Incident Response

If an online-safety concern is identified:

Is a child potentially at risk of harm?

YES → Report immediately to the DSL/deputy DSL → Follow the Child Protection and Safeguarding Policy.

If illegal activity or content is suspected:

- do not investigate yourself;
- do not unnecessarily view or share the material;
- preserve available evidence;
- follow DSL advice;
- contact appropriate safeguarding or law-enforcement agencies where required.

If there is no immediate safeguarding risk but the matter involves inappropriate use:

- report through the appropriate school procedure;
- record relevant details;
- consider behaviour, acceptable-use, disciplinary or technical responses;
- provide appropriate support; and
- review whether wider action is required.

Following significant incidents:

- review filtering and monitoring where relevant;
 - identify safeguarding learning;
 - consider curriculum implications;
 - consider staff-training needs;
 - inform governors through appropriate anonymised reporting; and
 - update policy or practice where necessary.
-