



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Contents

1. Introduction	2
2. Aims	3
3. Scope	4
4. Legislative Framework	5
4.1 Definitions	7
5. Roles and Responsibilities	9
5.1 Governing Board	10
5.2 Headteachers	10
5.3 Designated Safeguarding Lead (DSL)	11
5.4 Technical Support and IT Management	12
5.5 Staff 12	
5.6 Pupils	13
5.7 Parents and Carers	13
6. Online Safety Education	14
6.1 Staff Training	15
6.2 Parent and Carer Engagement	15
7. Managing Online Risks	16
7.1 Cyberbullying	17
7.2 Online Abuse, Exploitation and Harm	17
7.3 Nude and Semi-Nude Images	17
7.4 Artificial Intelligence (AI)	18
7.5 Emerging Technologies	18
8. Filtering and Monitoring	19
8.1 Filtering	19
8.2 Monitoring	20
8.3 Roles and Responsibilities	20
8.4 Responding to Alerts	21
8.5 Review of Filtering and Monitoring	22
9. Use of Technology and Digital Services	22
9.1 Federation Devices and Networks	22
9.2 Personal Devices	23
9.3 Artificial Intelligence (AI)	23
9.4 Photography, Audio and Video Recording	24
9.5 Online Communication	24
10. Online Communication and Social Media	25
10.1 Official Federation Communication	25
10.2 Staff Use of Social Media	26
10.3 Parents and Carers	26
10.4 Pupils' Use of Social Media	27
10.5 Responding to Online Concerns	27
11. Cyber Security and Information Protection	28
11.1 Cyber Security Measures	28



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

11.2 Information Protection	28
11.3 Cyber Security Awareness	29
11.4 Reporting Cyber Security Incidents	29
11.5 Business Continuity	30
12. Reporting, Responding to and Recording Online Safety Concerns	30
12.1 Reporting Concerns	30
12.2 Responding to Concerns	31
12.3 Recording Concerns	32
12.4 Working with External Agencies	32
12.5 Complaints	33
12.6 Monitoring and Review	33
Supporting Appendices	34
Appendix A – Online Safety Incident Response Guide	35
Appendix B – Filtering and Monitoring Review Process	39
Appendix C – Staff Online Safety Quick Reference Guide	40
Appendix D – Parent and Carer Online Safety Guidance	43
Appendix E – National Organisations and Sources of Support	45

1. Introduction

The Flourish Federation is committed to providing a safe, secure and supportive learning environment in which all members of the school community can benefit from the educational opportunities offered by digital technology whilst being protected from potential harm.

Technology plays an integral role in teaching, learning, communication and school administration. The Federation recognises that the online world presents significant opportunities to enhance learning, creativity, collaboration and personal development. However, it also presents risks including exposure to inappropriate content, online abuse, cyberbullying, misinformation, harmful online influences, exploitation, fraud and breaches of privacy.

Online safety is therefore viewed as a safeguarding responsibility rather than solely a technical or ICT matter. Effective online safety relies upon a whole-school approach involving leadership, governance, staff, pupils, parents and carers, alongside appropriate technical measures and a strong culture of vigilance.

This policy sets out how the Federation promotes safe, responsible and respectful use of technology, fulfils its statutory safeguarding duties, and responds proportionately to online safety concerns. It should be read alongside the Federation's:



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- Safeguarding and Child Protection Policy;
- Acceptable Use of Technology Policy;
- Behaviour Policy;
- Staff Code of Conduct;
- Data Protection Policy;
- Remote Learning procedures;
- Anti-Bullying Policy; and
- Relevant curriculum policies.

This policy applies to all members of the school community, including governors, employees, volunteers, contractors, pupils, parents and carers where their actions relate to the Federation or its pupils.

The Federation recognises that technology continues to evolve rapidly. This policy is therefore intended to provide overarching principles and expectations which will be supported by operational procedures and guidance where appropriate.

2. Aims

The aims of this policy are to:

- safeguard pupils and adults from harm associated with the use of digital technology and online services;
- promote a culture in which technology is used safely, responsibly, respectfully and lawfully;
- ensure that online safety is embedded within the Federation's safeguarding arrangements and forms part of everyday practice;
- enable pupils to develop the knowledge, skills and judgement required to navigate an increasingly digital world safely and confidently;
- ensure that staff understand their responsibilities for maintaining online safety and responding appropriately to concerns;
- provide clear expectations regarding the appropriate use of digital technologies, online platforms and Artificial Intelligence (AI);
- ensure appropriate filtering, monitoring and technical security measures are implemented and regularly reviewed;
- support parents and carers in promoting safe and responsible technology use beyond the school environment;



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- ensure that online safety concerns are identified, recorded, managed and escalated in accordance with safeguarding procedures;
- protect the Federation's information, systems and digital infrastructure from misuse, unauthorised access and cyber threats;
- promote compliance with relevant safeguarding, data protection and cyber security requirements; and
- support continuous improvement through regular monitoring, review and staff training.

3. Scope

This policy applies to all members of The Flourish Federation community, including:

- governors;
- employees;
- agency staff;
- volunteers;
- contractors;
- pupils;
- visitors using Federation technology or networks; and
- parents and carers where their actions relate to the Federation, its pupils or members of the school community.

The policy applies to:

- all Federation-owned digital devices and equipment;
- personally owned devices where their use relates to Federation business or activities;
- wired and wireless Federation networks;
- cloud-based services and online learning platforms;
- email systems;
- websites and social media associated with the Federation;
- Artificial Intelligence (AI) tools used for educational or professional purposes;
- remote learning environments;
- educational visits where digital technology is used; and
- any online activity that may affect the safety, wellbeing or reputation of pupils, staff or the Federation.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

The Federation recognises that online safeguarding concerns frequently originate away from school premises. Where online behaviour occurring outside school has the potential to:

- place a child at risk of harm;
- affect the safety or wellbeing of members of the school community;
- constitute bullying or harassment;
- involve criminal behaviour;
- disrupt the orderly running of the Federation; or
- bring the Federation into disrepute,

the matter will be considered in accordance with the Federation's safeguarding, behaviour and disciplinary procedures, taking account of the Federation's statutory responsibilities and powers.

This policy should be read alongside the Federation's Acceptable Use of Technology Policy, which sets out the detailed expectations for the day-to-day use of Federation technology and digital systems.

4. Legislative Framework

This policy has been developed with regard to current legislation, statutory guidance and recognised good practice, including but not limited to:

Primary Legislation

- Malicious Communications Act 1988;
- Children Act 1989;
- Computer Misuse Act 1990;
- Human Rights Act 1998;
- Education Act 2002;
- Communications Act 2003;
- Children Act 2004;
- Education and Inspections Act 2006;
- Equality Act 2010;
- Protection of Freedoms Act 2012;
- Data Protection Act 2018;
- UK General Data Protection Regulation (UK GDPR);
- Online Safety Act 2023; and



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- Children's Wellbeing and Schools Act 2026, where applicable.

Statutory Guidance

The Federation has particular regard to:

- *Keeping Children Safe in Education* (DfE), current edition;
- *Working Together to Safeguard Children*;
- *Relationships Education, Relationships and Sex Education (RSE) and Health Education*;
- *Searching, Screening and Confiscation*;
- *Behaviour in Schools*;
- *Teaching Online Safety in Schools*;
- *Meeting Digital and Technology Standards in Schools and Colleges*;
- *Filtering and Monitoring Standards for Schools and Colleges*;
- *Cyber Security Standards for Schools and Colleges*; and
- guidance issued by the Department for Education, the National Cyber Security Centre (NCSC), UK Safer Internet Centre and the Information Commissioner's Office (ICO), where relevant.

The Federation will review this policy whenever there are significant legislative or statutory changes affecting online safety, safeguarding or the use of technology within education.

Relationship with Other Policies

This policy should be read alongside, and operates in conjunction with, the Federation's:

- Safeguarding and Child Protection Policy;
- Acceptable Use of Technology Policy;
- Behaviour Policy;
- Anti-Bullying Policy;
- Data Protection Policy;
- Staff Code of Conduct;
- Dignity at Work Policy;
- Remote Learning procedures;
- Whistleblowing Policy;
- Disciplinary Policy; and
- relevant curriculum policies.

Where there is any conflict between this policy and statutory safeguarding guidance, the statutory guidance will take precedence.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

4.1 Definitions

The following definitions are provided to support understanding of the terminology used within this policy. They are intended as general explanations and should be read alongside current statutory guidance where applicable.

For the purposes of this policy, the following definitions apply:

Artificial Intelligence (AI)

Artificial Intelligence (AI) refers to computer systems or software capable of generating content, analysing information, recognising patterns or completing tasks that would normally require human intelligence. This includes generative AI tools that can produce text, images, audio, video or computer code.

Cyberbullying

Cyberbullying is the use of digital technology, online platforms or electronic communication to intentionally harass, intimidate, threaten, humiliate or target another person. Cyberbullying may occur through messaging services, social media, gaming platforms, email or other digital technologies.

Cyber Security

Cyber security refers to the measures taken to protect digital systems, devices, networks and information from unauthorised access, attack, damage, loss or disruption.

Digital Footprint

A digital footprint is the record of information, content and activity that an individual leaves through their use of digital technology. This may include social media activity, photographs, comments, search history, online purchases and other digital interactions, many of which may remain accessible long after they were created.

Digital Reputation



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Digital reputation refers to how an individual or organisation is perceived based on their online presence and behaviour. Content shared online may influence future educational, employment and personal opportunities.

Filtering

Filtering is the use of technology to restrict or block access to online content that is illegal, harmful or inappropriate, while allowing access to suitable educational resources.

Monitoring

Monitoring is the use of technology or processes to identify digital activity that may indicate a safeguarding concern, breach of policy or cyber security risk. Monitoring supports safeguarding but does not replace staff supervision or professional judgement.

Online Safety

Online safety is the safe, responsible, respectful and lawful use of digital technology. It includes protecting individuals from online harm whilst enabling them to benefit from the educational and social opportunities that technology provides.

Personal Devices

Personal devices are privately owned digital devices, including mobile phones, tablets, laptops, smart watches and similar technology, that are not owned or managed by the Federation.

Phishing

Phishing is a form of cybercrime in which fraudulent emails, messages or websites attempt to deceive users into revealing passwords, financial information or other sensitive data.

Safeguarding

Safeguarding, within the context of online safety, refers to protecting children from abuse, neglect, exploitation and harm that may occur through the use of digital technology or online services, and taking appropriate action where concerns arise.

Sextortion



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Sextortion is a form of online abuse in which an individual is coerced, manipulated or blackmailed into sharing intimate images, money or other material through threats, intimidation or exploitation.

Synthetic Media (Deepfakes)

Synthetic media, including deepfakes, refers to images, audio or video that have been created or manipulated using Artificial Intelligence or other digital technology to realistically depict events or individuals that did not occur or to alter genuine content.

Nude and Semi-Nude Images

The term *nude and semi-nude images* refers to images or videos created, shared or possessed by children that depict nudity or partial nudity. Incidents involving such images are managed in accordance with current statutory guidance and safeguarding procedures.

Technical Controls

Technical controls are the digital security measures used by the Federation to reduce online risks. They include filtering, monitoring, user permissions, authentication, software updates, antivirus protection and other cyber security measures.

5. Roles and Responsibilities

Maintaining online safety is a shared responsibility. While specific duties differ according to role, every member of the Federation community has a responsibility to contribute to a safe, secure and respectful digital environment.

The Governing Board, Headteachers, Designated Safeguarding Leads (DSLs), staff, pupils, parents and carers all play an important role in promoting online safety, preventing harm and responding appropriately to concerns.

Online safety arrangements are embedded within the Federation's wider safeguarding culture and are supported through effective leadership, education, appropriate technology, clear procedures and partnership working.

The responsibilities set out below should be read alongside the Federation's Safeguarding and Child Protection Policy and Acceptable Use of Technology Policy.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

5.1 Governing Board

The Governing Board has strategic responsibility for ensuring that effective online safety arrangements are in place across the Federation.

Governors will:

- ensure that appropriate online safety policies are adopted, implemented and reviewed;
- ensure that online safety forms part of the Federation's safeguarding arrangements;
- satisfy themselves that appropriate filtering and monitoring systems are in place, effective and regularly reviewed;
- receive regular assurance regarding the effectiveness of online safety arrangements, including the annual review of filtering and monitoring required by current DfE standards;
- ensure that sufficient resources are available to support effective online safety education, staff training and technical security;
- ensure appropriate oversight of cyber security and information security risks affecting the Federation;
- monitor compliance with relevant legislation and statutory guidance;
- provide appropriate challenge and support to senior leaders regarding online safety arrangements;
- promote a culture in which safeguarding, digital resilience and responsible technology use are prioritised; and
- ensure that online safety remains a standing consideration within the Federation's wider safeguarding governance.

Governors will receive appropriate training to enable them to understand their strategic responsibilities in relation to online safety, safeguarding, filtering and monitoring, and cyber security.

5.2 Headteachers

The Headteachers have overall operational responsibility for implementing this policy and ensuring that effective online safety arrangements are embedded throughout the Federation.

The Headteachers will:



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- promote a culture where online safety is recognised as an integral aspect of safeguarding;
- ensure appropriate leadership oversight of online safety across both schools;
- ensure suitable filtering and monitoring systems are implemented, maintained and regularly reviewed;
- ensure online safety risks are identified, assessed and managed appropriately;
- ensure concerns are responded to promptly and proportionately in accordance with safeguarding procedures;
- ensure staff receive appropriate induction and regular online safety training;
- ensure pupils receive progressive online safety education through the curriculum and wider personal development opportunities;
- ensure parents and carers are supported through appropriate communication and guidance;
- oversee the secure procurement, implementation and use of digital technologies;
- ensure cyber security risks are identified and appropriately managed;
- ensure appropriate risk assessments are undertaken before introducing new technologies or Artificial Intelligence (AI) tools;
- work closely with the DSL, technical support providers and governors to monitor the effectiveness of online safety arrangements; and
- ensure that lessons learned from incidents are used to strengthen practice, procedures and staff awareness.

Overall accountability for online safety remains with the Headteachers, although operational responsibilities may be delegated where appropriate.

5.3 Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) has lead responsibility for the safeguarding aspects of online safety and will work closely with senior leaders, technical support providers and staff to ensure that online risks are appropriately managed.

The DSL will:

- act as the lead professional for online safeguarding matters;
- ensure that online safety is fully integrated within the Federation's safeguarding procedures;
- receive, assess, record and manage online safety concerns in accordance with safeguarding procedures;
- make referrals to external agencies where appropriate;
- work with technical support providers where safeguarding concerns require investigation or technical intervention;



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- maintain oversight of emerging online risks and trends affecting children;
- support staff in managing online safety incidents involving pupils;
- ensure appropriate safeguarding records are maintained;
- contribute to staff training and pupil education regarding online safety;
- work in partnership with parents and carers where online safety concerns arise; and
- ensure that lessons learned from incidents inform future safeguarding practice.

5.4 Technical Support and IT Management

Those responsible for the Federation's technical infrastructure will support the safe, secure and effective operation of digital systems.

Technical support providers will:

- maintain appropriate filtering and monitoring systems;
- implement appropriate cyber security measures;
- ensure software, devices and operating systems are appropriately updated;
- support the secure management of user accounts and access permissions;
- investigate technical concerns where requested by senior leaders or the DSL;
- maintain appropriate backup and recovery arrangements;
- support regular testing of filtering and monitoring systems;
- support compliance with data protection and information security requirements;
- promptly report any safeguarding or cyber security concerns to senior leaders; and
- provide technical advice to support the Federation's ongoing online safety arrangements.

Technical staff are not responsible for determining safeguarding outcomes but will work alongside safeguarding leaders where technical evidence or intervention is required.

5.5 Staff

All staff share responsibility for promoting online safety and modelling safe, professional and responsible use of technology.

Staff will:

- comply with this policy and the Federation's Acceptable Use of Technology Policy;
- maintain appropriate professional boundaries when using digital technologies;
- promote safe, responsible and respectful online behaviour;
- deliver online safety education appropriate to pupils' age and stage of development;
- supervise pupils appropriately when technology is being used;



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- remain vigilant to signs of online abuse, exploitation or other safeguarding concerns;
- report online safety concerns immediately in accordance with safeguarding procedures;
- participate in mandatory online safety and safeguarding training;
- use only authorised systems, software and platforms for Federation business;
- ensure that personal data is processed securely and lawfully; and
- exercise professional judgement when using emerging technologies, including Artificial Intelligence (AI).

5.6 Pupils

Pupils are expected to use technology safely, responsibly and respectfully.

Pupils will:

- follow staff instructions regarding the safe use of technology;
- comply with age-appropriate acceptable use expectations;
- treat others respectfully when communicating online;
- protect their passwords and personal information;
- report any online content or behaviour that makes them feel unsafe or uncomfortable;
- respect the privacy and digital rights of others;
- use Federation technology only for authorised educational purposes; and
- understand that misuse of technology may result in sanctions in accordance with the Behaviour Policy and Acceptable Use of Technology Policy.

5.7 Parents and Carers

Parents and carers play an essential role in supporting children's safe and responsible use of technology.

The Federation encourages parents and carers to:

- promote safe and responsible technology use at home;
- engage positively with online safety guidance provided by the Federation;
- encourage children to speak openly about their online experiences;
- support age-appropriate use of devices, games, applications and social media;
- monitor and supervise children's online activity where appropriate;
- report concerns affecting pupils' safety or wellbeing to the Federation promptly;
- reinforce the Federation's expectations regarding respectful online behaviour; and
- work in partnership with the Federation to address online safety concerns.



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Where parents or carers communicate with the Federation using digital platforms or Artificial Intelligence (AI), they remain responsible for the accuracy, appropriateness and content of any information submitted.

6. Online Safety Education

The Federation is committed to developing pupils who are able to use technology safely, responsibly, respectfully and critically. Online safety education is embedded within the curriculum and wider school life, recognising that developing digital resilience is an ongoing process rather than a one-off event.

Online safety education is delivered through a combination of computing, Relationships Education, PSHE, assemblies, themed events, pastoral support and responsive teaching where emerging issues arise.

Teaching will be age-appropriate and adapted to reflect pupils' stage of development, local context and emerging online risks.

Online safety education will include, where appropriate:

- keeping personal information safe online;
- creating and managing secure passwords;
- recognising online grooming and exploitation;
- cyberbullying and respectful online communication;
- privacy settings and digital footprints;
- identifying scams, phishing and online fraud;
- misinformation, disinformation and fake news;
- healthy relationships online;
- consent, image sharing and appropriate online behaviour;
- age restrictions and responsible use of games, apps and social media;
- critical evaluation of online content;
- understanding how online activity contributes to an individual's digital reputation and future opportunities;
- the safe and ethical use of Artificial Intelligence (AI);
- balanced and healthy use of technology, including screen time and wellbeing;
- reporting concerns and seeking trusted adult support;
- understanding that online actions can have real-world consequences; and



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- understanding how to participate positively, respectfully and responsibly as digital citizens.

Staff will remain responsive to emerging issues and will adapt teaching where local, national or global events indicate that additional education is required.

The Federation recognises that online safety is most effective when reinforced consistently across the curriculum rather than delivered solely through isolated lessons.

6.1 Staff Training

All staff will receive appropriate online safety training as part of safeguarding induction and through regular updates thereafter.

Training will be proportionate to role and will include, where appropriate:

- current online safeguarding risks;
- recognising indicators of online abuse or exploitation;
- filtering and monitoring arrangements;
- professional conduct online;
- cyber security awareness;
- data protection responsibilities;
- appropriate use of Artificial Intelligence (AI);
- responding to online safety incidents; and
- changes to legislation and statutory guidance.

Additional training will be provided where new technologies or emerging risks are identified.

6.2 Parent and Carer Engagement

The Federation recognises that parents and carers play a vital role in promoting online safety beyond the school day.

The Federation will seek to support parents and carers by:

- providing online safety information and guidance;
- sharing advice on current online risks and emerging technologies;
- signposting trusted external resources;
- promoting Safer Internet Day and other national awareness campaigns;
- encouraging positive dialogue between parents and children about online activity; and
- working collaboratively with families where concerns arise.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

The Federation encourages parents and carers to report concerns promptly so that appropriate advice, support or safeguarding action can be taken where necessary.

7. Managing Online Risks

The online environment is continually evolving and presents both opportunities and risks for children and young people. The Federation recognises that online harms may occur within school, at home or elsewhere and that incidents occurring outside school may still require a safeguarding response where they affect the safety or wellbeing of pupils or members of the school community.

The Federation adopts a preventative, educative and safeguarding-led approach to managing online risks. Responses will always be proportionate to the nature of the concern and will take account of the child's age, understanding, vulnerability and individual circumstances.

Online risks may include, but are not limited to:

- cyberbullying, harassment and online abuse;
- online grooming and child sexual exploitation;
- child criminal exploitation;
- coercion, manipulation and sextortion;
- the creation, sharing or possession of nude or semi-nude images;
- exposure to harmful, violent, extremist or age-inappropriate content;
- misinformation, disinformation and manipulated media;
- online fraud, phishing and financial scams;
- identity theft and impersonation;
- excessive or unhealthy technology use;
- inappropriate online contact from adults or peers;
- risks associated with gaming, livestreaming and social media;
- misuse of Artificial Intelligence (AI), including the generation of inappropriate, harmful or misleading content;
- breaches of privacy or personal information; and
- cyber security incidents that may place individuals or the Federation at risk.

The Federation will provide appropriate education, supervision, technical safeguards and pastoral support to reduce these risks and will respond promptly where concerns arise.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

7.1 Cyberbullying

Cyberbullying is regarded as bullying and will be addressed in accordance with the Federation's Behaviour Policy and Anti-Bullying Policy.

Where cyberbullying affects members of the Federation community, staff will:

- investigate concerns promptly;
- provide appropriate support to those affected;
- apply sanctions where appropriate and proportionate;
- involve parents and carers where necessary;
- consider safeguarding implications; and
- involve external agencies where criminal offences or significant safeguarding concerns are suspected.

7.2 Online Abuse, Exploitation and Harm

Staff will remain vigilant to indicators that a pupil may be experiencing online abuse or exploitation.

Concerns may include:

- online grooming;
- sexual exploitation;
- criminal exploitation;
- coercion or blackmail;
- exposure to harmful online communities;
- radicalisation;
- online challenges presenting a risk of harm;
- repeated contact from unknown adults; or
- significant changes in a child's behaviour linked to online activity.

Any safeguarding concerns will be managed in accordance with the Federation's Safeguarding and Child Protection Policy. Where appropriate, referrals will be made to Children's Social Care, the police or other relevant agencies.

7.3 Nude and Semi-Nude Images

The Federation will respond to incidents involving the creation, possession or sharing of nude or semi-nude images in accordance with current statutory guidance.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Staff will never intentionally view or forward indecent images of children unless there is no reasonable alternative to safeguard a child. Any such incidents will be managed by the Designated Safeguarding Lead, with support from external agencies where required.

Pupils involved in such incidents will be treated as potentially vulnerable children who may require safeguarding support rather than automatic disciplinary action. The Federation will carefully consider the circumstances of each case before determining any sanctions.

7.4 Artificial Intelligence (AI)

The Federation recognises that Artificial Intelligence (AI) technologies are increasingly accessible and may present both educational opportunities and safeguarding risks.

Pupils will receive age-appropriate education regarding the safe, ethical and responsible use of AI.

The Federation will take appropriate action where AI is used to:

- generate abusive, discriminatory or harmful content;
- create, manipulate or distribute synthetic images, audio or video (including deepfakes) without consent;
- facilitate bullying or harassment;
- support academic dishonesty;
- impersonate another individual;
- circumvent safeguarding measures; or
- undertake any activity that places others at risk.

Further expectations regarding the use of AI are set out within the Federation's Acceptable Use of Technology Policy.

7.5 Emerging Technologies

The Federation recognises that technology develops rapidly and that new platforms, applications and devices may present previously unidentified safeguarding risks.

Senior leaders will monitor emerging technologies and, where necessary:

- undertake appropriate risk assessments;
- review safeguarding procedures;
- update curriculum content;
- provide additional staff training;



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- communicate with parents and carers; and
- implement additional technical controls where appropriate.

The absence of specific reference to a technology within this policy does not imply that its use is permitted or considered risk free. The principles of safeguarding, responsible behaviour and lawful use apply to all current and future technologies.

8. Filtering and Monitoring

The Federation recognises that filtering and monitoring systems are an important component of safeguarding arrangements but do not replace effective leadership, staff vigilance, education or professional judgement.

Appropriate filtering and monitoring systems will be implemented to help protect pupils and staff from accessing harmful or inappropriate content and to identify potential safeguarding concerns. These systems form part of the Federation's wider safeguarding strategy and are regularly reviewed to ensure they remain effective and proportionate.

The Federation will ensure that filtering and monitoring arrangements:

- are appropriate to the age and needs of pupils;
- comply with current statutory guidance and recognised good practice;
- support teaching and learning while minimising unnecessary restrictions;
- are capable of identifying potential safeguarding concerns;
- are reviewed regularly to reflect emerging risks and technological developments; and
- are supported by clear reporting and escalation procedures.

The Federation recognises that no filtering or monitoring solution can provide complete protection. Staff supervision, professional curiosity and safeguarding vigilance remain essential irrespective of the effectiveness of technical controls.

8.1 Filtering

Filtering systems are designed to reduce the likelihood of users accessing inappropriate, harmful or illegal online content.

Filtering arrangements will:

- block access to illegal content;



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- restrict access to age-inappropriate or harmful material;
- support compliance with safeguarding and legal requirements;
- allow appropriate educational access where justified;
- be regularly reviewed and tested; and
- be amended where emerging safeguarding risks are identified.

Requests to unblock or permit access to websites or online services for legitimate educational purposes will be considered by authorised staff following an assessment of educational value, safeguarding implications and cyber security risks.

8.2 Monitoring

Monitoring systems are used to identify activity that may indicate a safeguarding concern, breach of policy or cyber security risk.

Monitoring may identify, for example:

- attempts to access inappropriate content;
- concerning search terms;
- repeated attempts to bypass filtering controls;
- indicators of bullying, abuse or exploitation;
- attempts to access harmful or extremist material;
- misuse of Federation systems or accounts;
- cyber security threats; or
- other activity requiring investigation.

Monitoring information will be reviewed by appropriately authorised personnel and acted upon in accordance with the Federation's safeguarding procedures.

Monitoring systems are intended to support safeguarding and the secure operation of Federation systems. They are not used to routinely monitor staff performance or professional practice.

8.3 Roles and Responsibilities

The Governing Board will:

- receive assurance that appropriate filtering and monitoring arrangements are in place;
- ensure that filtering and monitoring form part of the Federation's safeguarding oversight; and



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- receive updates regarding significant risks, incidents or developments.

The Headteachers will:

- ensure filtering and monitoring systems remain appropriate and effective;
- ensure appropriate operational oversight;
- ensure concerns are investigated and managed appropriately; and
- report significant matters to governors where appropriate.

The Designated Safeguarding Lead (DSL) will:

- receive safeguarding concerns arising from monitoring where appropriate;
- assess identified risks;
- determine safeguarding responses;
- maintain appropriate safeguarding records; and
- liaise with external agencies where necessary.

Technical support providers will:

- maintain filtering and monitoring systems;
- investigate technical issues;
- support the implementation of agreed changes; and
- promptly report safeguarding or cyber security concerns to senior leaders.

8.4 Responding to Alerts

Where filtering or monitoring systems identify activity that may present a safeguarding concern, the Federation will respond promptly and proportionately.

Responses may include:

- reviewing the context of the activity;
- speaking with the pupil or member of staff where appropriate;
- informing the Designated Safeguarding Lead;
- contacting parents or carers where appropriate;
- implementing additional support or education;
- applying sanctions where misuse is identified;
- making referrals to external agencies where required; or
- reviewing technical controls to reduce future risk.



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Not all alerts indicate inappropriate behaviour. Each concern will be considered on its individual merits, taking account of context, intent and any safeguarding implications.

8.5 Review of Filtering and Monitoring

Filtering and monitoring arrangements will be reviewed regularly and whenever:

- significant safeguarding incidents occur;
- new technologies or online services are introduced;
- there are changes to statutory guidance;
- vulnerabilities or cyber security concerns are identified; or
- the Federation's safeguarding risk assessment indicates that changes are required.

The Governing Board will receive periodic assurance that filtering and monitoring arrangements remain effective, proportionate and appropriate to the needs of the Federation.

9. Use of Technology and Digital Services

The Federation promotes the safe, responsible and effective use of digital technology to enhance teaching, learning and communication. All users are expected to use technology in a manner that is lawful, professional, respectful and consistent with the Federation's values.

Detailed expectations relating to the day-to-day use of Federation technology are set out within the Federation's Acceptable Use of Technology Policy. This section outlines the key principles that underpin those expectations.

9.1 Federation Devices and Networks

Federation-owned devices, networks and digital services are provided primarily to support education, safeguarding and the effective operation of the Federation.

Users are expected to:

- use Federation technology for authorised purposes;
- protect login credentials and passwords;
- take reasonable care of equipment;
- report faults, damage or security concerns promptly;



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- avoid attempting to bypass security measures or filtering systems;
- access only systems and information for which they are authorised; and
- comply with all relevant Federation policies when using digital technology.

The Federation reserves the right to investigate suspected misuse of its systems where this is necessary to safeguard pupils, protect information, investigate misconduct or comply with legal obligations.

9.2 Personal Devices

The use of personal devices by staff, pupils, volunteers and visitors will be managed in accordance with the Federation's Acceptable Use of Technology Policy and any relevant local procedures.

Where personal devices are permitted, users must ensure that they:

- do not compromise safeguarding;
- do not compromise the security of Federation systems or information;
- are used appropriately and professionally; and
- comply with data protection requirements.

The Federation may place restrictions on the use of personal devices where this is necessary to protect pupils, staff or information security.

9.3 Artificial Intelligence (AI)

The Federation recognises the increasing availability of Artificial Intelligence (AI) technologies and their potential to support learning, administration and professional practice.

AI may be used where its use:

- supports educational objectives;
- enhances efficiency without replacing professional judgement;
- complies with safeguarding, data protection and copyright requirements;
- protects confidential and personal information;
- maintains academic integrity; and
- aligns with the Federation's Acceptable Use of Technology Policy.

Users remain responsible for any content created, edited or submitted using AI technologies.



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

AI-generated material should be reviewed for accuracy, appropriateness and potential bias before it is relied upon or shared.

Users remain accountable for decisions made using AI-assisted content and must not rely upon AI outputs without appropriate professional review.

The Federation does not permit the use of AI in ways that:

- create or distribute harmful, offensive or discriminatory content;
- facilitate bullying, harassment or intimidation;
- generate misleading or deliberately false information;
- circumvent assessment expectations or academic honesty;
- compromise safeguarding;
- infringe copyright or intellectual property rights; or
- breach data protection legislation.

9.4 Photography, Audio and Video Recording

The creation and use of photographs, audio recordings and video recordings must comply with the Federation's safeguarding, data protection and acceptable use requirements.

Users must not:

- record individuals without appropriate authority or consent where required;
- share images or recordings through unauthorised platforms;
- use recordings in a manner that may cause distress, embarrassment or harm; or
- edit or manipulate images in a way that misrepresents individuals or compromises safeguarding.

The use of cameras, mobile phones and recording devices during educational visits or school events will be managed in accordance with Federation procedures.

9.5 Online Communication

Digital communication between staff, pupils and parents or carers must take place only through authorised Federation systems, platforms or communication channels.

Staff must maintain appropriate professional boundaries at all times and must not use personal social media accounts or personal messaging services to communicate with pupils.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

All users are expected to communicate respectfully, professionally and in accordance with the Federation's Behaviour Policy, Staff Code of Conduct, Dignity at Work Policy and Acceptable Use of Technology Policy.

10. Online Communication and Social Media

The Federation recognises that online communication and social media provide valuable opportunities to engage with pupils, parents, carers and the wider community. However, their use must always support safeguarding, maintain professional standards and protect the reputation of the Federation.

All online communication associated with the Federation must be respectful, lawful and consistent with the Federation's values and policies.

10.1 Official Federation Communication

Official communication with parents, carers and the wider community will take place only through authorised Federation communication channels.

These may include:

- the Federation website;
- approved parental communication platforms;
- Federation email accounts;
- authorised social media accounts; and
- other systems approved by the Headteachers.

Official accounts will:

- be appropriately managed and monitored;
- publish accurate and appropriate information;
- protect the privacy of pupils and staff;
- comply with data protection requirements; and
- support positive engagement with the school community.



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

10.2 Staff Use of Social Media

Staff are expected to maintain the highest standards of professionalism when using social media or other online platforms.

Staff must:

- maintain appropriate professional boundaries at all times;
- avoid communicating with pupils through personal social media accounts or personal messaging services;
- avoid publishing material that could undermine public confidence in their professional role or the reputation of the Federation;
- ensure that personal opinions are not presented as those of the Federation;
- protect confidential information at all times; and
- comply with the Staff Code of Conduct, Acceptable Use of Technology Policy and relevant safeguarding procedures.

The Federation recognises that staff are entitled to a private life. However, conduct outside the workplace may become a disciplinary matter where it has the potential to affect safeguarding, professional standards or the reputation of the Federation.

10.3 Parents and Carers

The Federation encourages positive and constructive online engagement between home and school.

Parents and carers are expected to:

- communicate respectfully with members of the school community;
- avoid publishing material that is abusive, defamatory, discriminatory or deliberately misleading;
- respect the privacy of pupils, families and staff;
- raise concerns through the Federation's published procedures rather than through social media; and
- avoid sharing photographs or videos of other children without appropriate permission.

Parents and carers remain responsible for the content of anything they publish online or submit to the Federation, including material that has been drafted or assisted by Artificial Intelligence (AI).



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Where online activity by parents or carers has the potential to:

- compromise safeguarding;
- amount to harassment or intimidation;
- breach confidentiality;
- interfere with the operation of the Federation; or
- damage the reputation of individuals or the Federation,

the Federation may take appropriate action, including requesting removal of material, restricting communication channels where lawful and proportionate, reporting concerns to relevant platforms or agencies, or taking other action available within its legal powers.

10.4 Pupils' Use of Social Media

The Federation recognises that many pupils engage with online platforms and digital communication outside school.

Through the curriculum and wider safeguarding work, pupils will be supported to:

- communicate respectfully online;
- understand the permanence of digital content;
- protect their personal information;
- critically evaluate online information;
- recognise online manipulation and harmful influences;
- seek help where they experience inappropriate online behaviour; and
- understand the legal and personal consequences of online actions.

Where pupils' online behaviour outside school has a safeguarding impact, constitutes bullying, affects members of the school community or disrupts the orderly running of the Federation, the matter may be addressed through the Federation's safeguarding and behaviour procedures.

10.5 Responding to Online Concerns

The Federation will not routinely engage in public debate through social media regarding individual pupils, families, members of staff or complaints.

Concerns raised online will be considered on their merits and, where appropriate, individuals will be directed to the Federation's published complaints, safeguarding or communication procedures.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

The Federation reserves the right to retain evidence of online communications where necessary to support safeguarding, complaints, disciplinary processes or legal proceedings.

11. Cyber Security and Information Protection

The Federation recognises that effective cyber security is essential to safeguarding, protecting personal information, maintaining business continuity and ensuring the safe operation of digital systems.

Cyber security is regarded as a whole-organisation responsibility and requires the active participation of governors, leaders, staff, technical support providers and all users of Federation technology.

11.1 Cyber Security Measures

The Federation will implement proportionate technical and organisational measures to reduce cyber security risks.

These measures include, where appropriate:

- secure user authentication and password management;
- multi-factor authentication for supported systems;
- appropriate user access controls and permissions;
- secure disposal or recycling of digital equipment and storage media;
- regular software, firmware and security updates;
- antivirus and endpoint protection;
- secure network configuration;
- encrypted transmission of sensitive information where appropriate;
- secure backup arrangements;
- disaster recovery and business continuity planning;
- vulnerability management; and
- regular review of cyber security arrangements.

The Federation will seek technical advice where specialist expertise is required.

11.2 Information Protection

All users are responsible for protecting Federation information and personal data.



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Users must:

- access information only where authorised;
- protect usernames, passwords and authentication credentials;
- store information securely;
- follow Federation procedures for handling confidential information;
- report suspected data breaches immediately;
- avoid sharing confidential information through unauthorised platforms or personal accounts; and
- comply with the Federation's Data Protection Policy and relevant legislation.

11.3 Cyber Security Awareness

Staff and governors will receive appropriate cyber security awareness training as part of their induction and through ongoing professional development.

Training may include:

- recognising phishing emails;
- password security;
- multi-factor authentication;
- secure handling of information;
- identifying cyber threats;
- safe use of cloud services;
- secure home working; and
- reporting cyber incidents.

The Federation encourages all staff to remain vigilant to evolving cyber threats.

11.4 Reporting Cyber Security Incidents

Any suspected cyber security incident must be reported immediately to the Headteacher or other designated senior leader.

Examples include:

- suspected phishing attempts;
- malware or ransomware;
- compromised user accounts;
- unauthorised access to systems;
- loss or theft of Federation devices;



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- suspected data breaches;
- unusual system behaviour; or
- accidental disclosure of confidential information.

Where appropriate, the Federation will:

- isolate affected systems;
- seek technical support;
- assess safeguarding implications;
- comply with any statutory reporting requirements;
- notify affected individuals where required; and
- review procedures to reduce the likelihood of recurrence.

11.5 Business Continuity

The Federation maintains arrangements to support the continuity of education and school operations in the event of significant disruption to digital systems.

Business continuity and disaster recovery arrangements will be reviewed periodically to ensure they remain effective and proportionate.

12. Reporting, Responding to and Recording Online Safety Concerns

The Federation encourages a culture in which all members of the school community feel confident to report online safety concerns promptly. Early reporting enables concerns to be assessed, appropriate support to be provided and risks to be managed before they escalate.

All online safety concerns will be taken seriously and responded to proportionately, taking account of the nature of the concern, the age and needs of those involved, and any safeguarding implications.

12.1 Reporting Concerns

Any member of the school community who becomes aware of an online safety concern should report it immediately or as soon as reasonably practicable.

Concerns may relate to, but are not limited to:



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

- cyberbullying or online harassment;
- online grooming or exploitation;
- inappropriate contact from adults or peers;
- exposure to harmful, illegal or inappropriate content;
- the creation, possession or sharing of nude or semi-nude images;
- misuse of Artificial Intelligence (AI);
- breaches of this policy or the Acceptable Use of Technology Policy;
- cyber security incidents;
- misuse of Federation systems or devices; or
- any online activity that places a child or member of staff at risk.

Concerns relating to online abuse, harassment, intimidation or malicious online communications directed towards members of staff will be taken seriously and managed through the Federation's safeguarding, behaviour, complaints or disciplinary procedures as appropriate.

Staff must report safeguarding concerns immediately to the Designated Safeguarding Lead (DSL) in accordance with the Federation's Safeguarding and Child Protection Policy.

12.2 Responding to Concerns

The Federation will respond promptly and proportionately to all reported concerns.

Responses may include:

- speaking with those involved;
- securing relevant evidence where appropriate;
- assessing any immediate safeguarding risk;
- involving parents or carers where appropriate;
- implementing additional education or pastoral support;
- applying sanctions in accordance with the Behaviour Policy or staff disciplinary procedures;
- reviewing technical controls;
- making referrals to external agencies; and
- taking any other action necessary to safeguard children or protect Federation systems.

The welfare of the child will remain the Federation's paramount consideration when responding to online safeguarding concerns.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

12.3 Recording Concerns

Online safety concerns that have safeguarding implications will be recorded on the Federation's safeguarding recording system in accordance with the Safeguarding and Child Protection Policy.

Records will be:

- factual and contemporaneous;
- proportionate to the concern;
- stored securely;
- shared only with those who have a legitimate professional need to know; and
- retained in accordance with statutory guidance and the Federation's records management procedures.

Technical records may also be retained where necessary to support safeguarding, disciplinary procedures, complaints or legal processes.

12.4 Working with External Agencies

Where appropriate, the Federation will work collaboratively with external agencies to safeguard children and manage significant online safety concerns.

Depending on the nature of the concern, this may include:

- Children's Social Care;
- the Police;
- the Local Authority;
- the Local Authority Designated Officer (LADO);
- the Information Commissioner's Office (ICO);
- the Regional Cyber Crime Unit;
- the National Crime Agency (NCA);
- Child Exploitation and Online Protection (CEOP);
- health professionals; and
- other relevant safeguarding partners.

Referrals will be made in accordance with statutory safeguarding guidance and local safeguarding partnership procedures.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

12.5 Complaints

Concerns relating to online safety may be raised through the Federation's Complaints Policy where appropriate.

Safeguarding concerns, allegations against staff and concerns that may indicate a child is at risk of harm will not be managed solely through the complaints process and will instead be dealt with in accordance with the Federation's safeguarding procedures and relevant statutory guidance. Concerns will not normally be discussed through social media or other public online forums.

12.6 Monitoring and Review

The Headteachers and Governing Board will monitor the effectiveness of this policy through:

- review of safeguarding information;
- analysis of online safety incidents and trends;
- filtering and monitoring reviews;
- staff and pupil feedback;
- updates to statutory guidance;
- cyber security reviews; and
- governor oversight.

This policy will be reviewed annually, or sooner where there are significant changes to legislation, statutory guidance, technology or the Federation's safeguarding arrangements.

The review process will also consider changes in legislation, statutory guidance, technological developments, cyber security threats, Artificial Intelligence (AI), emerging online risks and lessons learned from incidents to ensure that the policy remains current, proportionate and effective.

The Flourish Federation recognises that technology will continue to evolve. By working in partnership with pupils, parents, carers, staff, governors and external agencies, the Federation aims to foster a culture in which technology is used safely, responsibly and positively, enabling all members of the school community to benefit from the opportunities of the digital world while remaining protected from harm



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Supporting Appendices

The appendices to this policy provide practical guidance and operational tools to support consistent implementation. They form part of this policy but may be updated independently where operational practice changes without affecting the substantive policy.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Appendix A – Online Safety Incident Response Guide

Purpose

This guide provides staff with a clear process for responding to online safety concerns. It supports, but does not replace, the Federation's Safeguarding and Child Protection Policy or professional judgement.

Step 1 – Identify the concern

An online safety concern may include, but is not limited to:

- cyberbullying or online harassment;
- inappropriate online communication;
- online grooming or exploitation;
- sextortion or online blackmail;
- the creation, sharing or possession of nude or semi-nude images;
- exposure to harmful, illegal or extremist content;
- concerning online searches or activity;
- misuse of Artificial Intelligence (AI);
- deepfake or manipulated images or videos;
- cyber security incidents; or
- any online activity that causes concern for a child's safety or wellbeing.



Step 2 – Is there an immediate risk of harm?

Yes

Take immediate safeguarding action.

- Inform the Designated Safeguarding Lead (DSL) immediately.
- If a child is in immediate danger, contact emergency services.
- Preserve any available evidence where it is safe and lawful to do so.
- Do not delay action whilst gathering further information.

Proceed in accordance with the Federation's Safeguarding and Child Protection Policy.

No

Proceed to Step 3.





The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Step 3 – Preserve the facts

Where appropriate:

- record exactly what has been observed or reported;
- retain screenshots or digital evidence if this can be done safely and lawfully;
- note dates, times and usernames where known;
- avoid altering or forwarding digital material unnecessarily.

Staff should not conduct their own investigation beyond establishing the basic facts.



Step 4 – Report the concern

Report the concern without delay to the appropriate person.

Concern	Report to
Child safeguarding concern	Designated Safeguarding Lead (DSL)
Staff safeguarding concern	Headteacher / DSL
Cyber security incident	Headteacher and Technical Support Provider
Suspected data breach	Headteacher / Data Protection Lead
Criminal activity	DSL (who will determine external referrals)



Step 5 – Assessment

The appropriate senior leader will assess:

- immediate safeguarding risk;
- welfare of those involved;
- whether parents or carers should be informed;
- whether technical investigation is required;
- whether external agencies should be involved;
- whether behaviour or disciplinary procedures apply; and
- whether additional support or education is required.



Step 6 - Respond



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Depending upon the circumstances, actions may include:

- safeguarding support;
- pastoral support;
- behaviour sanctions;
- restorative work;
- online safety education;
- technical intervention;
- amendment of filtering or monitoring arrangements;
- referral to Children's Social Care;
- referral to the Police;
- referral to CEOP;
- referral to the Local Authority;
- referral to the LADO (where allegations relate to staff); or
- no further action following assessment.



Step 7 - Record

Ensure that:

- safeguarding concerns are recorded on the Federation's safeguarding system;
- technical actions are documented where appropriate;
- records are factual, proportionate and contemporaneous; and
- confidential information is shared only with those who need to know.



Step 8 – Review & Learn

Following any significant incident, consider:

- Were safeguarding procedures effective?
- Were filtering and monitoring arrangements sufficient?
- Does the curriculum require updating?
- Is further staff training needed?
- Are parents or carers requiring additional guidance?
- Should technical controls be strengthened?
- Does this policy require amendment?

Lessons learned should be used to strengthen the Federation's safeguarding culture and online safety arrangements.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Key Principles

When responding to any online safety concern, staff should remember:

- **Safeguarding comes first.**
- **Do not investigate beyond your role.**
- **Do not promise confidentiality.**
- **Record facts, not opinions.**
- **Report concerns promptly.**
- **When in doubt, speak to the Designated Safeguarding Lead (DSL).**



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Appendix B – Filtering and Monitoring Review Process

Purpose

The Federation maintains a separate Filtering and Monitoring Review Record to document the regular review of its filtering and monitoring arrangements.

This operational document supports compliance with the Department for Education's *Filtering and Monitoring Standards for Schools and Colleges* and provides evidence of governance oversight.

Review Arrangements

Filtering and monitoring arrangements will be reviewed:

- at least annually;
- following any significant safeguarding or cyber security incident;
- following substantial changes to the Federation's technology infrastructure;
- when new technologies or digital services are introduced; and
- where changes to legislation or statutory guidance require a review.

Matters Considered

The review record will include consideration of:

- the effectiveness of filtering arrangements;
- the effectiveness of monitoring systems;
- safeguarding incidents arising from online activity;
- cyber security incidents;
- changes to statutory guidance;
- emerging online risks, including Artificial Intelligence (AI);
- staff training requirements;
- technical updates and improvements;
- actions arising from previous reviews; and
- recommendations for further improvement.

Governance

The review should involve, where appropriate:

- the Headteacher;
- the Designated Safeguarding Lead (DSL);
- the Federation's technical support provider; and
- a nominated governor with responsibility for safeguarding or digital oversight.

The completed review record will be retained by the Federation as evidence of compliance and will inform future improvements to online safety arrangements.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Appendix C – Staff Online Safety Quick Reference Guide

Purpose

This guide provides staff with a concise summary of their responsibilities for promoting online safety and responding to online safety concerns. It should be read alongside the Federation's Safeguarding and Child Protection Policy, Acceptable Use of Technology Policy and Staff Code of Conduct.

Everyday Expectations

All staff are expected to:

- use Federation technology safely, responsibly and professionally;
- maintain appropriate professional boundaries at all times;
- communicate with pupils only through authorised Federation systems;
- protect usernames, passwords and confidential information;
- supervise pupils appropriately when technology is being used;
- remain vigilant to online safeguarding risks;
- model safe and respectful online behaviour; and
- report concerns promptly.

If You Have an Online Safety Concern

Do

- ✓ Remain calm.
- ✓ Listen carefully and reassure the child where appropriate.
- ✓ Record factual information.
- ✓ Preserve evidence where appropriate and lawful.
- ✓ Report concerns immediately to the Designated Safeguarding Lead (DSL).
- ✓ Follow safeguarding procedures.

Do Not

- ✗ Investigate beyond your role.
- ✗ Promise confidentiality.
- ✗ Delete or alter evidence.



The Flourish Federation

Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

X Forward inappropriate images or content unless specifically instructed as part of safeguarding procedures.

X Attempt to resolve significant safeguarding concerns alone.

Examples of Concerns That Must Be Reported

Report immediately if you become aware of:

- online grooming;
- cyberbullying;
- sextortion;
- sharing of nude or semi-nude images;
- harmful online challenges;
- extremist or terrorist content;
- online coercion or exploitation;
- concerning online searches;
- misuse of Artificial Intelligence (AI);
- deepfake or manipulated images involving pupils or staff;
- cyber security incidents;
- online harassment of staff; or
- any online behaviour that places a child or member of staff at risk.

Safe Use of Artificial Intelligence (AI)

When using AI:

- use only approved systems for Federation business;
- never upload confidential or personal information into unauthorised AI tools;
- check AI-generated content for accuracy and bias;
- exercise professional judgement at all times;
- remain responsible for any work produced using AI; and
- report any inappropriate or unsafe use of AI.

Cyber Security Reminders

Always:

- lock your device when unattended;
- use strong passwords and multi-factor authentication where available;
- report suspicious emails immediately;
- keep confidential information secure;
- avoid using unauthorised software or websites; and
- report lost or stolen devices without delay.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Remember:

Online safety is everyone's responsibility.

If you are unsure whether something is a safeguarding concern:

Speak to the Designated Safeguarding Lead immediately.

It is always better to seek advice than to delay reporting.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Appendix D – Parent and Carer Online Safety Guidance

Purpose

The Federation recognises that parents and carers play a vital role in helping children develop the knowledge, skills and confidence to use technology safely and responsibly.

Online safety is most effective when home and school work together to promote positive digital habits, encourage open communication and respond promptly to concerns.

Supporting Your Child Online

Parents and carers are encouraged to:

- take an active interest in their child's online activities;
- talk regularly about the websites, games, apps and online services they use;
- encourage children to tell a trusted adult if something online worries or upsets them;
- establish age-appropriate boundaries for the use of devices and online services;
- make use of parental controls and privacy settings where appropriate;
- supervise younger children's online activity;
- encourage respectful and responsible online behaviour;
- discuss the permanence of digital footprints and online reputation;
- help children understand that not everything online is accurate or trustworthy; and
- reinforce the importance of protecting personal information and passwords.

Artificial Intelligence (AI)

Artificial Intelligence (AI) is becoming an increasingly common part of everyday life. Parents and carers are encouraged to:

- discuss with their child how AI tools can be used safely and responsibly;
- remind children that AI-generated information may be inaccurate or misleading;
- encourage children to think critically rather than accepting AI-generated content without question; and
- support the school's expectations regarding the appropriate use of AI for learning.

If Your Child Experiences an Online Safety Concern

If your child experiences an online safety concern:

- remain calm and listen carefully;
- reassure them that they have done the right thing by speaking to you;
- avoid deleting evidence where it may be needed;
- report abusive content using the relevant platform where appropriate;
- contact the Federation if the concern affects your child's safety, wellbeing or school life; and
- contact the Police immediately if there is an immediate risk of harm or criminal activity.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Working in Partnership

The Federation asks parents and carers to:

- communicate respectfully with members of the school community;
- raise concerns through the Federation's published procedures rather than through social media;
- avoid sharing photographs or videos of other children without appropriate permission;
- respect the privacy of pupils, families and staff; and
- work collaboratively with the Federation to support children's safety and wellbeing.

Parents and carers remain responsible for the content of any material shared online or submitted to the Federation, including material that has been drafted or assisted by Artificial Intelligence (AI).

Further Information

Further advice and support is available from the organisations listed in **Appendix E – National Organisations and Support**.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Appendix E – National Organisations and Sources of Support

Purpose

The following organisations provide reliable information, advice and support relating to online safety, safeguarding, cyber security and digital wellbeing. They may be used by the Federation, staff, parents, carers and pupils to access additional guidance where appropriate.

Safeguarding and Child Protection

Child Exploitation and Online Protection (CEOP)

Provides advice and support regarding online child sexual abuse and exploitation. CEOP also enables concerns about online grooming or exploitation to be reported.

NSPCC

Provides safeguarding advice for children, parents and professionals, including guidance on online safety, social media, gaming and digital wellbeing.

Childline

Offers free, confidential advice and support for children and young people experiencing online or offline concerns.

Online Safety

UK Safer Internet Centre

Provides guidance, educational resources and advice for schools, professionals, parents and young people on staying safe online.

Internet Matters

Offers practical guidance for parents on parental controls, online safety, gaming, social media and emerging technologies.

Common Sense Media

Provides age-based reviews of apps, games, films, websites and digital services to help families make informed choices.



The Flourish Federation Online Safety Policy

Ratified	15 th July 2026	Review	July 2027
----------	----------------------------	--------	-----------

Cyber Security

National Cyber Security Centre (NCSC)

Provides guidance on cyber security, phishing, ransomware, password security, multi-factor authentication and protecting digital systems.

Action Fraud

The UK's national reporting centre for fraud, cybercrime and online scams.

Data Protection

Information Commissioner's Office (ICO)

Provides guidance relating to data protection, privacy rights, information security and UK GDPR compliance.

Government Guidance

The Federation has regard to current government guidance relating to online safety and safeguarding, including:

- *Keeping Children Safe in Education;*
- *Working Together to Safeguard Children;*
- *Teaching Online Safety in Schools;*
- *Filtering and Monitoring Standards for Schools and Colleges;*
- *Cyber Security Standards for Schools and Colleges;*
- *Meeting Digital and Technology Standards in Schools and Colleges;*
- *Searching, Screening and Confiscation;* and
- other relevant guidance published by the Department for Education.

Reporting Concerns

If a child is believed to be at immediate risk of harm, concerns should be reported without delay to the appropriate emergency services or Children's Social Care in accordance with the Federation's Safeguarding and Child Protection Policy.

Concerns relating to pupils attending the Federation should also be reported promptly to the Designated Safeguarding Lead (DSL).