Over St. John's C.E Primary School

'Let your light shine before others.' Matthew 5:16

Online Safety Policy

1.1 Introduction and purpose

At Over St. John's C.E. Primary School, we are committed to ensuring that all members of our school community are able to use digital technologies safely, responsibly and respectfully.

Online safety is an essential part of our wider safeguarding approach. It is embedded within our curriculum, reinforced through staff training and behaviour expectations, and supported by appropriate technical systems and clear reporting routes.

This policy sets out:

- our approach to online safety
- the responsibilities of staff, governors, pupils, parents and external partners
- how the school supports safe and effective use of technology
- how concerns and incidents are identified, reported and responded to

Our approach is informed by the safeguarding expectations of Cheshire West and Chester and by current national statutory guidance.

1.2 Scope

This policy applies to:

- all pupils
- all staff, including supply staff and volunteers
- governors
- parents and carers when engaging with the school digitally
- visitors and contractors
- community users granted access to school systems or devices

It applies to:

- school-owned devices and systems
- personal devices brought onto the school site where permitted
- school networks, internet services and platforms
- online activity taking place off site where it impacts the safety, wellbeing, behaviour or reputation of pupils, staff or the school community

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- RSHE Policy
- Staff Code of Conduct
- Data Protection Policy
- Acceptable Use Agreements

- Filtering and Monitoring procedures
- Mobile Device guidance
- Whistleblowing Policy
- Complaints Policy

1.3 Aims

The school aims to:

- keep children safe online
- help pupils develop the knowledge and skills needed to use technology positively and safely
- promote respectful, responsible and age-appropriate digital behaviour
- ensure staff model safe and professional online conduct
- maintain effective filtering, monitoring and technical security arrangements
- ensure concerns are reported, recorded and acted upon promptly
- work in partnership with parents, carers, governors and external agencies

1.4 Statutory and safeguarding framework

This policy has been written with reference to current statutory and non-statutory guidance, including:

- Keeping Children Safe in Education
- Working Together to Safeguard Children
- DfE Filtering and Monitoring Standards for Schools and Colleges
- DfE guidance on meeting digital and technology standards in schools and colleges
- DfE Cyber Security Standards
- Prevent duty guidance
- UK GDPR and data protection legislation
- relevant Cheshire West and Chester safeguarding partnership guidance

Online safety is treated as a safeguarding matter and is integrated within the school's wider child protection arrangements.

1.5 Roles and responsibilities

The governing body

The governing body will:

- approve and review this policy
- ensure that online safety is fully embedded within the school's safeguarding culture
- receive regular updates on online safety implementation, incidents and developments
- ensure that suitable filtering and monitoring arrangements are in place and reviewed
- support access to appropriate staff training
- appoint a named governor with responsibility for online safety

The headteacher

The headteacher will:

- take overall responsibility for the school's safeguarding culture, including online safety
- ensure this policy is implemented effectively
- support staff in following clear procedures when concerns arise
- work with the DSL, Online Safety Lead, governors and IT provider to ensure effective oversight
- ensure appropriate action is taken in relation to serious incidents

The Designated Safeguarding Lead

The DSL has overall lead responsibility for online safety as part of the safeguarding role. The DSL will:

- maintain oversight of online safety concerns and incidents
- ensure concerns are dealt with in line with safeguarding procedures
- work closely with the Online Safety Lead and IT provider

- ensure online safety is understood as part of the wider safeguarding picture
- consider when external agencies, including children's social care or the police, need to be involved
- ensure records are kept securely and appropriately

The Online Safety Lead

The Online Safety Lead will:

- support the DSL with day-to-day coordination of online safety
- monitor trends, incidents and emerging risks
- support development, review and implementation of this policy
- work with curriculum leaders to ensure online safety education is planned and progressive
- provide advice and support to staff as needed
- help organise staff, pupil and parent awareness activity
- support the review of acceptable use arrangements

Staff

All staff will:

- read, understand and follow this policy and related guidance
- complete safeguarding and online safety training as required
- model safe, respectful and professional online behaviour
- use school systems for communication with pupils and parents/carers
- supervise pupils appropriately when using digital technologies
- report concerns immediately through the school safeguarding procedures
- follow the school's acceptable use expectations
- be alert to risks such as grooming, cyberbullying, sexual harassment, extremism, misinformation and contact from unknown users

Pupils

Pupils are expected to:

- use technology safely, sensibly and respectfully
- follow staff instructions when using devices, the internet or school platforms
- tell an adult if they see or receive anything upsetting, suspicious or inappropriate
- not share personal information or images without permission
- behave online in ways that reflect the school's values

Parents and carers

Parents and carers are encouraged to:

- support the school's online safety messages at home
- supervise children's use of devices and online services outside school
- talk to children about safe and responsible online behaviour
- inform the school of any concerns that may affect a child's safety or wellbeing

The IT provider

The IT provider will:

- maintain secure systems and infrastructure
- support filtering, monitoring and access controls
- provide logs or reports where appropriate
- work with the DSL and senior leaders on reviews, checks and improvements
- ensure technical measures are aligned with safeguarding expectations

1.6 Teaching and learning

Online safety is taught as part of the school curriculum and reinforced across the wider life of the school. Pupils will learn about:

- being safe, kind and respectful online
- how to report concerns and seek help

- age-appropriate use of the internet and digital devices
- recognising online stranger risk and grooming behaviours
- cyberbullying, harassment and harmful online behaviour
- privacy, passwords and personal information
- misinformation, unreliable content and critical thinking
- safe use of apps, games and social media
- healthy screen habits and balance
- what to do if they are worried about something online

The curriculum will be:

- age-appropriate
- progressive across year groups
- adapted where necessary for pupils with SEND or additional vulnerabilities
- reviewed regularly to reflect emerging risks and curriculum needs

Online safety will be delivered through:

- Computing and online safety lessons
- PSHE
- assemblies
- themed days and national initiatives
- class discussion and wider curriculum links

1.7 Acceptable use of technology

The school requires all users to follow acceptable use expectations.

Users must not:

- access, create, share or store illegal, harmful or inappropriate material
- use school systems to bully, harass, threaten or discriminate against others
- bypass or attempt to bypass filtering, monitoring or security measures
- share passwords or access accounts without permission
- download, upload or install unauthorised software or content
- use school devices or networks for private business or personal gain
- breach copyright, data protection or confidentiality requirements
- use devices or platforms in ways that compromise the ethos, safety or reputation of the school

Separate acceptable use agreements will be provided for staff, pupils and, where relevant, community users.

1.8 Staff use of technology and professional conduct

Staff are expected to maintain high standards of professional behaviour online and offline.

Staff must:

- use school-approved systems for communication with pupils, parents and carers
- keep professional and personal communications separate
- not use personal social media, personal email or personal messaging accounts for school communication
- be mindful of their digital footprint and online reputation
- not post content that may bring the school into disrepute
- follow school guidance on taking, storing and sharing images and video
- report any accidental contact, concerning message or safeguarding issue immediately
- Staff are reminded that their conduct online may be scrutinised where it affects their professional role or the reputation and safeguarding of the school community.

1.9 Use of personal devices, images and social media

The school will maintain clear expectations regarding:

- mobile phones
- tablets and other personal devices
- photography and video
- social media use in school and relating to the school

The school will:

- clearly define where and when personal devices may be used
- ensure pupils understand when device use is not permitted
- only allow the taking and sharing of images in accordance with consent and school procedures
- ensure staff do not use personal devices in ways that compromise safeguarding or professionalism

Any image or recording used by the school will be obtained, stored and shared in line with consent, data protection and safeguarding requirements.

1.10 Filtering and monitoring

The school takes a robust approach to filtering and monitoring in line with DfE expectations.
The school will:

- maintain appropriate filtering and monitoring systems
- review the effectiveness of those systems at least annually and after any significant incident
- work collaboratively with the DSL, senior leaders, governors and IT provider
- ensure staff understand how to report concerns arising from filtering or monitoring
- adjust systems where necessary in response to risk, incidents or changes in technology

The school recognises that no system is completely effective on its own. Filtering and monitoring are supported by:

- staff vigilance
- curriculum education
- clear reporting routes
- a strong safeguarding culture

1.11 Reporting and responding to concerns

All members of the school community must report online safety concerns promptly.
Concerns may include:

- cyberbullying
- sexual harassment or sexual violence online
- inappropriate contact or grooming
- exposure to harmful or age-inappropriate content
- extremist or radicalising content
- sharing of images without consent
- misuse of school systems
- suspected illegal activity
- concerns about staff conduct

The school will:

- take all reports seriously
- act promptly and proportionately
- involve the DSL where safeguarding concerns are present
- preserve evidence where required
- not investigate serious illegal activity independently where this may compromise evidence or a police investigation
- record concerns and outcomes appropriately

Where there is a safeguarding concern, the school will follow child protection procedures. Where there is a concern about staff conduct, the headteacher and, where appropriate, the Chair of Governors will be informed.
Where necessary, the school will involve:

- parents and carers
- local authority safeguarding partners
- police
- social care
- specialist external support

1.12 Managing incidents
The school will respond to online safety incidents in line with the nature and seriousness of the concern.
Possible responses may include:

- restorative conversation
- education and guidance
- parental involvement
- restriction or removal of device access
- sanctions in line with the behaviour policy
- safeguarding referral
- involvement of external agencies

When dealing with incidents, staff will:

- remain calm and professional
- avoid asking leading questions
- preserve relevant evidence where appropriate
- record what was seen, heard or reported
- refer to the DSL without delay if a safeguarding concern is identified

1.13 Training and support
The school will ensure:

- staff receive online safety training at induction
- safeguarding and online safety updates are provided at least annually
- governors receive appropriate awareness and training
- the DSL and Online Safety Lead access further training to keep knowledge current
- training reflects emerging risks and statutory guidance

Additional support will be provided where needed for:

- new staff
- volunteers
- supply staff
- pupils with SEND
- parents and carers

1.14 Working with parents and carers
The school will support parents and carers through:

- information on the website
- newsletters and communications
- parent workshops or information sessions where possible
- signposting to reputable support and advice
- sharing key messages about safe device use, apps, games and social media

The school recognises that parents and carers are key partners in helping children stay safe online.

1.15 Record keeping, monitoring and review

The school will keep appropriate records of:

- online safety incidents
- filtering and monitoring checks
- staff training
- policy review
- curriculum delivery and developments

This policy will be:

- reviewed annually
- updated sooner if there are significant changes in statutory guidance, technology, risks or school practice

The governing body will receive regular information to support oversight and assurance.

1.16 Equality and inclusion

The school is committed to ensuring that online safety education and support are accessible to all pupils. We will consider:

- age and developmental stage
- SEND
- pupils with communication needs
- pupils with English as an additional language
- pupils who may be more vulnerable to exploitation, bullying or coercion online

Appendices

Appendix A (page 10) - Acceptable Use Agreements
Appendix B (page 15) - Reporting and Response Flowchart
Appendix C (page 20) - Incident Recording and Response Guidance
Appendix D (page 24) - Filtering and Monitoring Overview
Appendix E (page 27) - Useful External Support

Appendix A - Acceptable Use Agreements

A.1 School allowed / not allowed table

Area	**Allowed**	**Allowed with permission / at certain times**	**Not allowed**
Accessing the internet	For learning, research and school-related activities using approved systems	When directed by staff for a specific purpose	Accessing illegal, harmful or inappropriate content
Games	Educational games when linked to learning and approved by staff	Limited use in supervised settings where explicitly permitted	Games that are age-inappropriate, unsafe, violent, sexual, gambling-related or that encourage unsafe contact with others
Messaging and chat	Use of approved school platforms for learning and communication where necessary	Internal school communications under staff supervision	Unsanctioned chatting, messaging or contact with strangers
Social media	Where required by staff for official school purposes and in line with school procedures	For approved school promotion or curriculum use, under staff control	Personal use by pupils in school; using social media to bully, harass, pressure or share inappropriate content

Area	Allowed	Allowed with permission / at certain times	Not allowed
Email	Use of school email for legitimate school purposes by authorised users	Use of email by staff in line with professional expectations	Use of personal email for school business with pupils or parents
Online research	Research using websites that staff have checked or directed pupils to use	Broader searching when supervised by staff	Deliberate searching for inappropriate, harmful or illegal material
Video/audio	Using approved educational video or audio resources	Recording or broadcasting only when authorised and in line with consent	Live streaming, recording or sharing without permission
Mobile phones	Not used by pupils during the school day unless authorised	Staff mobile phones may be used in line with school expectations	Unauthorised use of mobile phones by pupils
Personal devices	Not used by pupils unless specifically authorised	Used by staff only where permitted by school policy	Bypassing school systems, accessing restricted content or creating safeguarding risks
Images and video	Taken and used only with permission and according to school procedures	Staff may use school-approved devices and systems for authorised purposes	Taking, sharing or posting images without consent or for personal use
Files and downloads	Downloading approved resources for school work	With staff permission and school systems	Installing unauthorised software, malware, games or files
Passwords and accounts	Secure use of individual school accounts	Password resets or access support through authorised staff	Sharing passwords or using another person's account
Conduct online	Respectful, kind and lawful behaviour	Reflection and support where mistakes are made	Bullying, harassment, discrimination, threats, impersonation or illegal activity

A.2 Staff acceptable use agreement

All staff, including supply staff, volunteers and temporary workers where relevant, must follow this agreement when using school systems, devices and accounts.

Staff must:

- use school digital systems responsibly, professionally and lawfully
- keep work and personal digital activity separate
- use school-approved systems for communication with pupils, parents and carers
- follow the school's safeguarding, behaviour, data protection and confidentiality expectations
- use strong passwords and keep login details secure
- log off and lock devices when not in use
- only use approved platforms and applications for school business
- report concerns, suspicious activity or policy breaches immediately to the DSL, headteacher or other designated senior leader
- model positive, respectful and safe online behaviour
- be mindful of their digital footprint, privacy settings and online reputation
- follow school procedures for storing, sharing and deleting files, images and recordings
- use school guidance when taking photographs or videos of pupils

- comply with copyright and licensing requirements
- ensure that any online communication is professional in tone and content

Staff must not:

- use personal email, personal messaging apps or personal social media accounts to communicate with pupils or parents about school matters
- access, store, create or share offensive, illegal or inappropriate material
- bypass or attempt to bypass filtering, monitoring or security systems
- share passwords or allow others to access their accounts
- use school systems for private business or personal gain
- take, share or post images, recordings or information in ways that breach safeguarding, consent or data protection requirements
- post or share anything online that could bring the school into disrepute
- engage in online behaviour that could undermine public confidence in the school or the profession

Professional expectations

Staff should remember that:

- online behaviour may have safeguarding, disciplinary or reputational consequences
- communications with pupils must always be appropriate, necessary and visible through approved school systems where relevant
- any accidental contact, concerning message or suspicious online activity must be reported without delay

Staff declaration

I confirm that I have read, understood and agree to follow the school's Staff Acceptable Use Agreement and Online Safety Policy.

Name: _____

Role: _____

Signature: _____

Date: _____

A.3 Pupil acceptable use agreement

This agreement should be shared with pupils in age-appropriate language. For younger pupils, staff may adapt the wording into a child-friendly version.

Pupils must:

- be kind, respectful and sensible when using technology
- only use devices, websites and apps when a member of staff says it is safe to do so
- tell a trusted adult straight away if anything online upsets, worries or confuses them
- keep personal information private
- never share passwords
- never pretend to be someone else online
- never take, send or share photos or videos without permission
- never use school technology to upset, exclude, bully or trick others
- follow staff instructions about logging on, saving work and logging off
- use the internet for school purposes only when directed by staff
- understand that school rules also apply when using technology at school events, on trips or through school systems

Pupils must not:

- search for or share harmful, violent, sexual or illegal content

- contact strangers online
- use school systems to send hurtful messages
- download or install games, apps or files without permission
- try to access blocked sites, bypass filters or use another person's account
- damage, change or delete other people's work
- use technology in a way that would upset others or bring the school into disrepute

Pupils should understand:

- that their online actions can affect real people
- that adults in school are there to help them stay safe
- that they can always report a concern without getting into trouble for speaking up

Pupil declaration

I agree to use school technology safely and to follow the school's online safety rules.

Name: _____

Class: _____

Signature: _____

Date: _____

A.4 Parent and community user expectations

Parents and carers

Parents and carers play an important role in helping children use technology safely. The school encourages parents and carers to:

- support the school's online safety messages at home
- talk to children regularly about their online activity
- supervise the use of devices, apps, games and websites at home
- understand age ratings, privacy settings and parental controls
- encourage children to tell an adult if they are worried about something online
- follow the school's expectations when communicating with staff digitally
- avoid posting or sharing material online that could identify, embarrass or harm pupils, staff or the school community

Parents and carers should be aware that:

- the school may respond to online behaviour outside school where it affects pupil safety, wellbeing or the orderly running of the school
- any online concern involving a child will be handled in line with safeguarding procedures where appropriate

Parent / carer declaration

I understand the school's online safety expectations and will support my child to use technology safely.

Name: _____

Signature: _____

Date: _____

Community users

Community users granted access to school systems, platforms, wifi or other resources must:

- use them only for the approved purpose
- follow the school's safeguarding, data protection and acceptable use expectations
- keep login details secure
- not share, copy or remove school information without permission
- report any concerns, misuse or technical issues immediately
- comply with any additional terms of use set by the school

Community user declaration
I agree to follow the school's acceptable use expectations and to use school systems only for the approved purpose.
Name: _____
Organisation / role: _____
Signature: _____
Date: _____

Appendix B - Reporting and Response Flowchart
B.1 Purpose
This appendix sets out the school's reporting and response route for online safety concerns. It is designed to help staff, volunteers, governors and other adults respond promptly and appropriately when an online safety issue arises.
B.2 Key principles
When an online safety concern is identified:

- do not ignore it
- do not delay
- do not investigate serious harm or illegal activity yourself
- do not promise confidentiality
- do not share the concern more widely than necessary
- do record and report promptly

B.3 Reporting route
If a pupil, staff member, volunteer, visitor or parent/carer is concerned about online content, conduct or contact, they should follow this route:
Step 1 - Identify the concern
The concern may involve:

- cyberbullying
- harmful or inappropriate content
- sexual harassment or sexual abuse online
- grooming or suspicious contact
- extremist or radicalising material
- sharing of images without consent
- misuse of school systems
- suspected illegal activity
- inappropriate staff conduct
- a technical or filtering issue

Step 2 - Stop and preserve
If safe to do so:

- stop further viewing, sharing or commenting
- do not delete the evidence
- do not forward harmful content unless instructed
- make a brief note of what was seen or heard

Step 3 - Report immediately
Report the concern to one of the following:

- the DSL
- the Online Safety Lead
- the headteacher

- another senior leader, if the above are unavailable

Where the concern involves a member of staff, report to the headteacher. If the concern involves the headteacher, report to the Chair of Governors.

Step 4 - Assess the level of concern

The DSL or senior leader will decide whether the issue is:

- a safeguarding concern
- a behaviour issue
- a staff conduct issue
- a technical issue
- a possible criminal matter

Step 5 - Take action

Action may include one or more of the following:

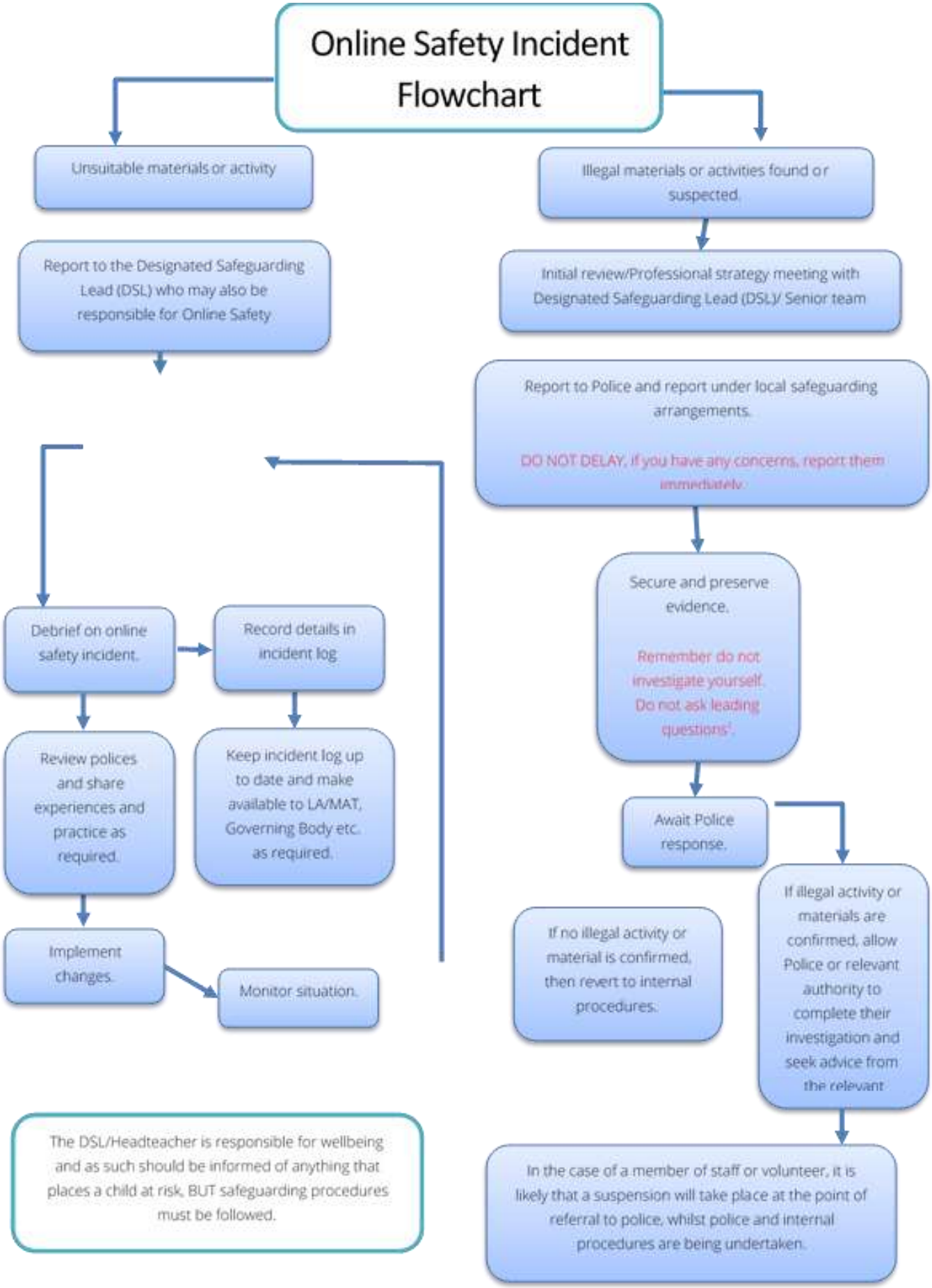
- speaking to the pupil, staff member or parent/carer
- applying school behaviour sanctions
- restricting or removing access to devices or systems
- recording the incident
- involving the DSL or headteacher
- contacting parents and carers
- making a referral to children's social care
- contacting the police
- seeking advice from the local authority or other external agencies

Step 6 - Record and review

The incident will be recorded on the school's incident log and reviewed to see whether:

- further safeguarding action is needed
- the curriculum needs strengthening
- staff training needs updating
- filtering or monitoring systems need adjustment

B.4 Flowchart



B.5 If illegal content or serious harm is suspected

If there is any suspicion of:

- child sexual abuse material
- grooming
- coercion or exploitation
- extremist content
- threats of violence
- serious harassment or stalking
- fraud or extortion
- hacking or cyber-crime
- non-consensual image sharing

then staff must:

- refer immediately to the DSL
- preserve evidence if it is safe to do so
- not carry out their own investigation
- follow safeguarding procedures
- seek police advice or involvement where appropriate

B.6 If the concern involves a pupil

Where the concern involves a pupil, staff should:

- respond calmly and reassure the pupil
- listen without leading questions
- avoid promising secrecy
- record the facts as soon as possible
- refer to the DSL
- involve parents and carers if appropriate and in line with safeguarding procedures

B.7 If the concern involves a member of staff

Where the concern involves a member of staff, staff should:

- report it immediately to the headteacher
- follow the school's safeguarding and whistleblowing procedures
- preserve any relevant evidence if safe to do so
- not discuss the matter with others unless authorised

Where the concern involves the headteacher, report to the Chair of Governors.

B.8 If the concern is a technical or filtering issue

Where the concern relates to:

- blocked content
- inappropriate access
- monitoring alerts
- account security
- suspected system misuse

staff should:

- report it to the DSL and IT provider
- record the issue
- avoid making changes themselves unless authorised
- follow any urgent safeguarding instructions

B.9 Post-incident follow-up

After any significant incident, the school may:

- review the pupil's support needs
- arrange staff reminders or training
- update filtering or monitoring settings
- revisit the curriculum offer
- inform governors of relevant anonymised learning
- update related policies or procedures

Appendix C - Incident Recording and Response Guidance

C.1 Purpose

This appendix sets out how online safety incidents should be recorded and responded to. It is intended to support consistent, proportionate and safeguarding-led practice across the school.

C.2 What should be recorded

Whenever an online safety concern is reported, the school should record:

- the date and time of the incident
- the name and role of the person reporting it
- who was involved
- what was seen, said or shared
- where the incident took place, if known
- which device, platform, app, website or system was involved
- the immediate action taken
- who was informed
- whether parents and carers were contacted
- whether the DSL, headteacher or other senior leader was informed
- whether any external agency was contacted
- the outcome of the incident
- any follow-up action or support

C.3 Recording standards

Records should be:

- factual
- concise
- objective
- written as soon as possible after the incident
- stored securely
- accessible only to those who need to know

Records should not:

- include speculation
- include emotive or judgemental language
- be shared unnecessarily
- be left on unsecured devices or in informal notes

C.4 Immediate response expectations

When a concern is reported, staff should:

- remain calm and professional
- reassure the pupil or adult reporting the concern
- avoid asking leading questions
- avoid investigating beyond what is necessary to secure the facts
- preserve evidence where appropriate
- refer to the DSL or senior leader promptly
- follow safeguarding procedures where there is any risk of harm

C.5 Evidence handling

Where it is safe and appropriate to do so, staff should:

- make a brief note of what was seen or heard
- record the URL, platform name or account details if relevant
- take a screenshot only if this is permitted and appropriate under school procedures
- avoid deleting content unless instructed to do so
- avoid forwarding harmful content unless there is a clear safeguarding reason

Staff must not:

- attempt to search for more harmful material than is necessary
- conduct their own investigation into illegal content
- share screenshots or images beyond those who need to know

C.6 Decision-making

The DSL, headteacher or other designated senior leader will decide whether the matter:

- can be managed through school behaviour procedures
- requires parental involvement
- requires internal safeguarding follow-up
- should be referred to children's social care
- should be referred to the police
- requires input from the IT provider or external technical support

C.7 Follow-up actions

Following an incident, the school may:

- provide reassurance and support to those affected
- put in place pastoral or safeguarding support
- increase supervision or monitoring
- restrict access to devices, platforms or systems
- update behaviour or safeguarding records
- inform staff of relevant learning in an anonymised way
- review whether curriculum content or staff training needs strengthening
- review whether filtering and monitoring systems need adjustment

C.8 Communication and confidentiality

Information about online safety incidents should be shared only:

with staff who need to know
with parents and carers where appropriate and in line with safeguarding
with external agencies where required
with governors in anonymised or summarised form where relevant

Staff should not discuss incidents informally with colleagues, pupils or families unless authorised to do so.

C.9 Retention and storage

Records should be retained and stored in line with the school's:

- safeguarding record-keeping procedures
- data protection policy
- retention schedule

Any digital record should be stored securely and not on personal devices or unsecured accounts.

C.10 Learning from incidents

The school will use anonymised information from incidents to:

- identify patterns or emerging risks

- update online safety teaching
- inform staff training
- review acceptable use expectations
- improve filtering, monitoring and technical controls
- strengthen safeguarding practice

Incident recording template
Online Safety Incident Record
Date of incident: _____
Time of incident: _____
Reported by: _____
Role of reporter: _____
Person(s) involved: _____
Year group / class, if relevant: _____
What was seen, said or shared?

Where did the incident happen?

Device / platform / website / app involved:

Immediate action taken:

Who was informed?

Was the DSL informed? Yes / No
Was the headteacher informed? Yes / No
Were parents and carers informed? Yes / No
Were any external agencies informed? Yes / No
If yes, please state: _____
Outcome of the incident:

Follow-up action / support required:

Name of staff member completing record:

Signature: _____
Date completed: _____

Appendix D - Filtering and Monitoring Overview

D.1 Purpose

This appendix explains the school's approach to filtering and monitoring. It sets out the responsibilities, expectations and review arrangements that help the school keep pupils and staff safe online.

D.2 Principles

The school recognises that:

- filtering and monitoring are essential safeguarding measures
- technical systems must be supported by staff vigilance and a strong safeguarding culture
- no system is completely effective on its own
- filtering and monitoring arrangements must be proportionate to the needs and risks of the school
- systems must be reviewed regularly and updated when risks change

D.3 What filtering and monitoring mean

Filtering

Filtering is the process of restricting access to inappropriate, harmful or illegal online content.

Monitoring

Monitoring is the process of checking the use of digital systems to identify:

- misuse
- unsafe activity
- safeguarding concerns
- technical issues
- patterns of risk

D.4 Responsibilities

Governing body

The governing body will:

- ensure that the school has appropriate filtering and monitoring systems in place
- receive regular updates about their effectiveness
- support annual review and oversight
- ensure that online safety remains part of wider safeguarding oversight

Headteacher and senior leaders

The headteacher and senior leaders will:

- work with the DSL and IT provider to oversee filtering and monitoring arrangements
- ensure systems are reviewed at least annually and after significant incidents
- ensure staff understand how to report concerns
- ensure that safeguarding concerns arising from monitoring are followed up appropriately
-

Designated Safeguarding Lead

The DSL will:

- hold overall safeguarding oversight of filtering and monitoring
- work closely with the Online Safety Lead and IT provider
- review concerns arising from filtering or monitoring
- decide whether concerns require safeguarding action
- ensure that patterns or trends are considered in safeguarding and curriculum planning

IT provider

The IT provider will:

- implement and maintain technical filtering and monitoring systems
- provide relevant reports or logs where required
- respond to technical issues and concerns

- support testing, review and adjustment of settings
- work with school leaders to ensure systems remain effective

Staff

All staff will:

- follow school procedures if they identify a concern about filtering or monitoring
- report accidental access to inappropriate content immediately
- supervise pupils appropriately when using technology
- avoid changing settings or bypassing controls unless authorised

D.5 School expectations

The school will:

- apply age-appropriate filtering across school systems
- block access to illegal, harmful and inappropriate content
- monitor online activity in a manner proportionate to safeguarding needs
- review monitoring alerts and concerns promptly
- keep a record of any issues identified and action taken
- ensure pupils are educated about the reasons for filtering and monitoring
- adjust systems when new risks or patterns emerge
-

D.6 Review process

Filtering and monitoring arrangements will be reviewed:

- at least annually
- after any significant online safety incident
- when there are changes to:
- technology
- safeguarding risk
- curriculum needs
- statutory guidance
- school systems or providers

The review should consider:

- whether blocked content is appropriate
- whether monitoring is effective
- whether staff know how to report concerns
- whether any new risks need additional controls
- whether the school's internet safety teaching needs strengthening

D.7 Reporting concerns

Concerns identified through filtering or monitoring may include:

- access attempts to inappropriate websites
- repeated searches for harmful content
- signs of grooming or exploitation
- misuse of school systems
- attempts to bypass controls
- technical faults affecting safety

Any concern should be reported to the DSL, Online Safety Lead or senior leader without delay.

D.8 Record keeping

The school will keep a record of:

- filtering and monitoring reviews

- concerns identified through systems
- actions taken
- changes made to settings or controls
- training or follow-up completed

Records should be stored securely and shared only with those who need to know.

D.9 Staff and pupil understanding

The school will make sure that:

- staff know what to do if a concern is identified
- pupils understand that online activity may be monitored for safety reasons
- parents and carers are aware that the school uses filtering and monitoring to safeguard children

D.10 Ongoing improvement

The school will use monitoring information to:

- identify trends and concerns
- inform staff development
- strengthen curriculum content
- improve safeguarding practice
- review and refine technical controls

Appendix E - Useful External Support

E.1 Purpose

This appendix provides a list of external organisations and support services that may be useful for pupils, parents and carers, staff and governors when dealing with online safety issues.

E.2 Support for children and young people

CEOP CEOP provides advice and support for children and young people who are worried about someone online, including grooming, exploitation or inappropriate contact.

Childline Childline offers confidential support for children and young people who want to talk about worries, including online bullying, harassment, unsafe contact or distressing content.

UK Safer Internet Centre The UK Safer Internet Centre provides online safety advice, resources and guidance for children, young people, parents and professionals.

E.3 Support for parents and carers

UK Safer Internet Centre - parent advice

Parents and carers can use this service for practical guidance on:

- parental controls
- apps and games
- social media
- screen time
- online risks
- talking to children about online safety

Childnet Childnet provides clear advice and resources for parents and carers on helping children stay safe online.

CEOP advice for parents and carers CEOP offers information for families on spotting the signs of online harm and reporting concerns.

E.4 Support for schools and staff

Reporting Harmful Content This service helps schools and staff report harmful online content and understand how to escalate concerns.

Local safeguarding partnership guidance The school will refer to Cheshire West and Chester safeguarding partnership guidance where relevant.

Police The police should be contacted where there is a concern about illegal content, threat, grooming, exploitation, serious harassment, extortion, hacking or other criminal activity.
Social care Children's social care should be contacted where an online issue raises safeguarding concerns about a child's welfare or safety.

E.5 Additional useful organisations
The school may also signpost to:

- Internet Watch Foundation
- NSPCC
- Professionals Online Safety Helpline
- Ofsted guidance where relevant to safeguarding reviews
- school or trust safeguarding materials

E.6 Guidance for use
The school will ensure that:

- families are signposted to appropriate support in a sensitive way
- pupils are encouraged to speak to a trusted adult if they are worried
- staff know which services are appropriate for different types of concern
- any referral to an external body is made in line with safeguarding procedures

Date created: September 2026
Approved by governors: September 2026
Next review date: September 2027
Policy owner: DSL- Emma Snowdon / Online Safety Lead – Emma Bettley
Responsible governor: Online Safety Governor - Hayley Rogers
School ICT Support - Matthew Beard
SCiE Team - Pam Beech