Fishergate Primary School

Online Safety Policy

Policy Date:	March 2026
Review Date:	March 2027

Approved by: Governing Body

Designated Safeguarding Lead (DSL): Tina Clarke

Policy Statement

At Fishergate Primary School, we recognise that technology and the internet play an important role in children's education, communication and social development. However, they also present risks which must be carefully managed.

The school is committed to ensuring that:

- Pupils are protected from harm online.
- Staff and pupils use technology safely, responsibly and respectfully.
- Online safety is embedded in the curriculum, safeguarding systems and school culture.
- Parents and carers are supported in keeping children safe online.

Aims

The aims of this policy are to:

- Protect pupils from online harm including cyberbullying, exploitation, grooming and exposure to harmful content.
- Ensure safe and responsible use of digital technologies within school.
- Provide clear guidance for staff, pupils, governors and parents.
- Establish procedures for responding to online safety incidents.
- Support pupils to develop digital resilience and responsible online behaviour.

Scope of the Policy

This policy applies to all members of Fishergate Primary School (pupils, teaching and support staff, governors, volunteers, contractors, visitors and parents and carers) and covers the use of:

- School devices
- Personal devices
- School networks
- Online platforms used for learning
- Digital communication with pupils or families

When interacting with our digital technologies both in school and where school technology or platforms are used outside school.

Online Safety Risks

Our approach to online safety focuses on addressing the following the Four Key Categories of Risk (KSIE):

- **Content** – exposure to illegal, inappropriate or harmful material, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – harmful interactions with others online, including peer pressure, commercial advertising, and adults posing as children or young people in order to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – a person's online behaviour that may increase the likelihood of harm or cause harm to others, such as creating, sending or receiving explicit images (including consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other inappropriate images, and engaging in online bullying.
- **Commerce** – risks associated with online financial activity, including online gambling, inappropriate advertising, phishing attempts and financial scams.

Roles and Responsibilities

Fishergate Primary School is a community and all members are expected to behave respectfully both online and offline. Technology should be used to support teaching and learning and to help prepare pupils for life beyond school. Any concerns or inappropriate behaviour must be reported to the DSL promptly to ensure the safeguarding of everyone in our community.

Governing Body

The governing body will:

- Ensure the school has appropriate online safety policies and procedures.
- Ensure the school meets safeguarding requirements under KCSIE.
- Understand the filtering and monitoring systems in place.
- Monitor the effectiveness of the policy.
- Ensure staff receive appropriate training.
- Ensure pupils are taught how to keep themselves and others safe, including online.

Headteacher

The Headteacher will:

- Ensure the policy is implemented effectively.
- Ensure online safety is integrated into safeguarding systems.
- Ensure staff receive regular training.

- Support the DSL (if not themselves) in managing online safety concerns.

Designated Safeguarding Lead (DSL)

The DSL will:

- Take lead responsibility for online safeguarding.
- Manage online safety incidents.
- Work with external agencies where necessary.
- Maintain records of incidents.
- Ensure staff understand reporting procedures.
- Provide staff guidance and training.
- Understand and monitor filtering and monitoring systems.

Staff

All staff (including volunteers and contractors) must:

- Understand the online safety is part of safeguarding and such, it is everyone's responsibility
- Model safe and responsible technology use.
- Follow the **Staff Acceptable Use Agreement** and ensure pupils follow the **Pupil Acceptable Use Agreement**.
- Report online safety incidents and concerns in line with the school behaviour policy
- Deliver online safety education as appropriate.

Pupils

Pupils are expected to:

- Use technology responsibly.
- Follow the **Pupil Acceptable Use Agreement**.
- Report anything that makes them feel unsafe or uncomfortable online.

Parents and Carers

Parents and carers are encouraged to:

- Support safe internet use at home.
- Monitor children's online activities at home.
- Report concerns to the school.
- Support the terms set out in the pupils' Acceptable Use Agreements

ICT Provider (Vital)

Vital manages our windows based system, Google workspace and provide the school with IT support.

Vital is responsible for managing our Google Drive, Chromebooks and iPads through:

- Providing reliable hardware, which is appropriate for education, (eg desktop PCs, laptops, Chromebooks or iPads) and associated peripherals

- The initial set-up, delivery, installation and disposal of all waste

- Ongoing support and personal service from an assigned technician

- Proactive and reactive technical support

- Accidental damage cover

- Providing advice and input on project work including refurbishments and moves

- Refreshing hardware every three years

- Putting in place an appropriate level of security protection, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting a full security check and monitoring the school's ICT systems on a regular basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Broadband Provider (North)

North is responsible for managing our broadband service on behalf of York City Council and City Fibre. They provide:

<u>Security, safeguarding and filtering</u>

· Internet filtering by group, user or device (Smoothwall)

· https inspection

· Layer 7 application control

· Firewall and intrusion prevention

· Configurable monitoring and reporting functions

· Antivirus and malware protection for web content

· Transparent proxy

· Remote access

· Site to site VPN

Service and maintenance

· Service desk, including site visits by DBS checked engineer when required

· Maintained equipment

· Service Level Agreement

· A proactive monitoring service

Online Safety Education

Online safety education is embedded throughout the curriculum and particularly through:

- Computing
- PSHE
- Relationships and Health Education

In line with the National Curriculum and RSE guidance, pupils are taught about:

- Safe internet use
- Protecting personal information
- Cyberbullying and respectful communication
- Recognising online risks
- Reporting concerns
- Age-appropriate digital behaviour

Teaching is adapted to be age appropriate across Key Stage 1 and Key Stage 2:

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

As part of Fishergate's commitment to raising the attainment of disadvantaged young people (RADY), these pupils' SEMH and wider academic needs are prioritised. Any barriers for disadvantaged pupils, including pupils from families seeking sanctuary, are overcome so they can participate fully in the Computing curriculum and achieve the above outcomes alongside their peers.

Online safety may also be reinforced through:

- Assemblies
- Workshops
- National awareness events (e.g. Safer Internet Day)

Purple Mash

At Fishergate Primary School, we use the Purple Mash scheme of work alongside supplementary resources from code.org, BBC Teach, Digital Matters, Thinkuknow, UK Safer Internet Centre.

Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) technologies are increasingly becoming used in education and online platforms. The school recognises both the opportunities and potential risks associated with AI tools.

As we introduce AI via Purple Mash units and/or other means, we will ensure that:

- AI tools used within school are appropriate for primary-aged pupils.
- Staff supervise and guide pupils in the responsible use of AI.
- AI systems do not compromise data protection or safeguarding requirements.
- Pupils understand that AI-generated content may not always be accurate.

Pupils will be taught to:

- Use AI tools responsibly.
- Check information sources critically.
- Understand that AI should not replace independent thinking or learning.

Staff must not:

- Enter personal or confidential pupil information into AI systems that are not approved by the school.
- Use AI tools in ways that compromise safeguarding or data protection.

Informing and Supporting Parents/Carers

The school works with parents/carers to promote online safety by:

- Providing online safety information on the school website and in newsletters
- Sharing guidance via newsletters
- Providing advice on parental controls and safe use of devices

Parents/Carers will be informed of:

- Online risks
- School expectations for technology use
- Procedures for reporting concerns.

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

- NSPCC
- Internet Matters
- UK Safer Internet Centre
- Childnet

Cyberbullying

Cyberbullying is defined as bullying behaviour that takes place using digital technologies.

This can include:

- Abusive messages
- Sharing images without consent
- Exclusion from online groups
- Impersonation
- Online harassment

To prevent and address cyber-bullying, the school will:

- Ensure pupils understand what it is and what to do if they are a victim or become aware of it happening to others
- Ensure all staff receive training on cyber-bullying
- Treat cyberbullying as a serious safeguarding issue.
- Investigate incidents promptly.
- Support victims.
- Apply appropriate sanctions in line with the behaviour policy.
- Involve parents and external agencies where necessary.
- Examine electronic devices where necessary

Examining Electronic Devices

The Headteacher, or a member of staff authorised by the Headteacher, may search and confiscate an electronic device if there are reasonable grounds to suspect that it:

- Poses a risk to pupils or staff
- Contains a banned item under school rules
- May contain evidence of a suspected offence

Before carrying out a search, staff will, where appropriate:

- Consider the urgency and any risk to pupils or staff, seeking advice from the Headteacher if needed
- Explain the reason for the search and how it will be conducted
- Allow the pupil to ask questions and seek their cooperation

Authorised staff may examine data or files on a confiscated device where there is good reason, for example if it may have been used to:

- Cause harm
- Disrupt the safe environment of the school or learning
- Commit an offence

In exceptional circumstances, staff may delete files where their continued existence may cause harm and the pupil or parent refuses to remove them. If the material may be evidence of a criminal offence, it will not be deleted and the device will be passed to the police.

If inappropriate material is found, the Headteacher will decide on the appropriate response. Safeguarding concerns will be addressed in line with the school's safeguarding procedures.

If staff suspect a device contains an indecent image of a child (nude or semi-nude image), they will:

- Not view the image (this is illegal)
- Confiscate the device
- Report the incident immediately to the Designated Safeguarding Lead (DSL)

All searches will follow:

- UK Department for Education guidance on *Searching, Screening and Confiscation*
- UK Council for Internet Safety guidance on *Sharing nudes and semi-nudes*
- The school's Behaviour Policy.

10. Acceptable Use

The school maintains Acceptable Use Agreements for:

- Staff
- Pupils
- Volunteers
- Governors

These agreements outline expectations for:

- Appropriate online behaviour
- Responsible use of school devices
- Protection of personal data
- Safe communication online

All pupils and staff must sign an acceptable use agreement and school will monitor the websites visited by all members of and visitors to the school.

11. Pupils Using Mobile Devices

At Fishergate Primary, pupils are not permitted to use mobile phones during the school day.

Where pupils bring mobile devices to school:

- Phones must be switched off and stored securely at the school office until the end of the school day.
- The school accepts no responsibility for loss or damage.

Pupils are not permitted to wear or use smartwatches in school. Children are allowed to use a step counter watch but nothing that can send/receive messages or calls, take photographs or access the internet.

12. Staff Use of Mobile Devices

Staff must:

- Use school laptops responsibly.
- Lock the device if leaving unattended.
- Keep operating systems up to date by always installing the 'push' updates.
- Never communicate with pupils through personal social media or messaging services.

- Use school-approved platforms for communication with families (e.g. Class Dojo)

Staff must not:

- Take photographs of pupils on personal devices.
- Store pupil data on personal phones.
- Use personal devices in ways that compromise safeguarding.

13. Responding to Online Safety Incidents

All online safety and/or safeguarding concerns must be reported to the Designated Safeguarding Lead.

The school will:

1. Record the incident
2. Investigate appropriately
3. Assess safeguarding risk
4. Take appropriate action

Actions may include:

- Supporting pupils
- Contacting parents
- Applying behaviour sanctions
- Reporting to external agencies
- In serious cases, contacting the police

Incidents will be recorded in the school's recording system (CPOMS).

14. Data Protection

The school handles personal data in accordance with data protection legislation.

Staff must:

- Protect confidential information
- Use secure systems
- Follow the school's data protection procedures.

15. Staff Training

Staff receive online safety training at least once a year as part of safeguarding training along with relevant updates as required throughout the academic year (e.g. emails, staff briefings or meetings).

Training includes:

- Awareness that online safety is a safeguarding issue and understanding their safeguarding responsibilities
- Technology can be used to facilitate abuse, exploitation and bullying.
- Understanding that pupils' online behaviour is treated with the same seriousness as other safeguarding concerns.
- Awareness of the four categories of online risk: content, contact, conduct and commerce.
- Responding to incidents
- Understanding filtering and monitoring
- Awareness of how to spot signs and symptoms of online abuse.

New staff receive online safety training as part of their induction.

Governors will receive safeguarding training including training on safe internet use and online safeguarding issues.

Volunteers will receive appropriate training if required.

16. Monitoring and Review

This policy will be:

- Reviewed **annually**
- Updated in line with changes in legislation or safeguarding guidance
- Approved by the Governing Body

The effectiveness of the policy will be monitored through:

- Safeguarding audits
- Incident logs
- Staff and pupil feedback
- Governor oversight.

Appendices

Appendix A – Staff Acceptable Use Agreement

Appendix B – Pupil Acceptable Use Agreement KS1

Appendix C – Pupil Acceptable Use Agreement KS2

Appendix D – Online Safety Incident Reporting Procedure

Appendix E – Guidance for Parents

Appendix F – Staff Quick Guide

Appendix G – Classroom Poster

Appendix A – Staff Acceptable Use Agreement

Staff Acceptable Use Agreement

All staff, volunteers and governors must agree to the following:

I agree that I will:

- Use school technology for professional purposes only.
- Protect confidential information and personal data.
- Follow school safeguarding and data protection policies.
- Report any online safety concerns to the DSL immediately.
- Maintain appropriate professional boundaries online.
- Use school-approved systems when communicating with pupils or parents.

I will not:

- Use personal devices to photograph or record pupils.
- Store pupil data on personal devices.
- Access, create or share inappropriate material using school systems.
- Communicate with pupils via personal social media accounts.

I understand that failure to follow this agreement may result in disciplinary action.

Name:
Signature:
Date:

Appendix B – Pupil Acceptable Use Agreement (KS1)

KS1 Pupil Acceptable Use Agreement

At Fishergate, we want everyone to stay safe online.

When I use computers, tablets or the internet at school, I promise that I will:

- Use it safely and responsibly.
- Ask for help if something happens that I don't understand
- Tell a teacher if something online makes me feel worried, upset or uncomfortable.
- Only visit websites that my teacher allows.
- Be kind and respectful when sending messages.
- Keep my QR code or Emoji password safe.

I will not:

- Try to access websites that are not allowed.
- Share personal information (name, address, phone number).
- Send unkind messages or images.
- Use someone else's account.

I understand that school can check my messages, files and the websites I visit.

I understand if I do not follow these rules, I may lose access to school technology.

Pupil Name:
Signature:
Date:

Appendix C – Pupil Acceptable Use Agreement (KS2)

KS2 Pupil Acceptable Use Agreement

At Fishergate, we want everyone to stay safe online.

When I use computers, tablets or the internet at school, I promise that I will:

- Use technology safely and responsibly.
- Ask for help if I see a pop up or something I don't understand.
- Tell a teacher if something online makes me feel worried, upset or uncomfortable.
- Only visit websites that my teacher allows.
- Be kind and respectful when communicating online.
- Keep my personal information private (name, address, phone number, passwords).

I will not:

- Try to access websites that are not allowed.
- Share personal information online.
- Send unkind messages or images.
- Use someone else's account.
- Install any software or hardware or use a memory stick without permission from a teacher.

I understand that school can check my messages, files and the websites I visit.

I understand that access to school technology and the internet is a privilege that requires responsibility and that if I do not follow these rules, I may lose access to school technology.

Pupil Name:
Signature:
Date:

Appendix D – Responding to Online Safety Incidents

Online Safety Incidents

When an online safety concern is reported, staff will:

1. Reassure the pupil and listen carefully.
2. Avoid promising confidentiality.
3. Record the concern accurately.
4. Report the concern to the Designated Safeguarding Lead.

The DSL will then:

- Assess the level of risk.
- Record the incident in safeguarding systems.
- Contact parents where appropriate.
- Seek advice from external agencies if necessary.
- Report serious incidents to relevant authorities.

Appendix E – Guidance for Parents

Parents and carers play an important role in keeping children safe online.

The school encourages parents to:

- Talk regularly with children about online safety.
- Use parental controls where appropriate.
- Monitor online activity and device use.
- Encourage children to speak up if they encounter problems online.

You can seek further guidance on keeping children safe online from the following organisations:

- NSPCC
- Internet Matters
- UK Safer Internet Centre
- Childnet

Parents should contact the school if they are concerned about a child's online safety.

Appendix E – Governor Online Safety Monitoring Checklist

Online Safety Monitoring Checklist

Governors play an important role in ensuring the effectiveness of online safety arrangements within the school.

Governors should regularly review the following:

Policy and Leadership

- The school has a current Online Safety Policy that is reviewed annually.
- Online safety is integrated within the safeguarding policy.
- A Designated Safeguarding Lead are clearly identified.

Filtering and Monitoring

Governors should understand:

- What filtering system the school uses.
- What monitoring systems are in place.
- Who reviews monitoring alerts.
- How often systems are reviewed.

Staff Training

Governors should ensure that:

- Staff receive regular safeguarding and online safety training.
- New staff receive online safety training during induction.

Curriculum

Governors should check that pupils are taught about:

- Safe internet use
- Online bullying
- Protecting personal information
- Reporting concerns

Incident Management

Governors should review anonymised information on:

- Online safety incidents
- Cyberbullying cases
- Safeguarding concerns involving online activity

Parental Engagement

Governors should ensure the school:

- Provides online safety guidance for parents
- Promotes awareness through the school website and/or newsletters

Technology and Risk Management

Governors should confirm that:

- School devices are secure and regularly updated.
- Personal data is protected.
- New technologies are risk assessed before being introduced.

Appendix F - Staff Quick Guide:

Staff Quick Guide

Online safety is part of our safeguarding responsibility. All staff must remain vigilant and respond to concerns in the same way as any other safeguarding issue.

Online Risks

Four Key Categories of Risk (from KSIE):

- **Content** – exposure to illegal, inappropriate or harmful material, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – harmful interactions with others online, including peer pressure, commercial advertising, and adults posing as children or young people in order to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – a person's online behaviour that may increase the likelihood of harm or cause harm to others, such as creating, sending or receiving explicit images (including consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other inappropriate images, and engaging in online bullying.
- **Commerce** – risks associated with online financial activity, including online gambling, inappropriate advertising, phishing attempts and financial scams.

Be alert if a pupil:

• Becomes secretive about online activity
• Shows distress after using devices
• Is receiving excessive messages or contact online
• Mentions online dares, challenges or threats
• Talks about people they only know online

If a pupil reports an online concern:

1. Listen calmly and take the concern seriously.
2. Reassure the pupil they have done the right thing.
3. Do NOT promise confidentiality.
4. Do NOT investigate or view images unnecessarily.
5. Record the concern accurately.
6. Report immediately to the Designated Safeguarding Lead (DSL).

Never:
• Ask a pupil to forward explicit images
• View, copy, store or share images
• Attempt to investigate incidents alone

Technology Use

Staff must:
• Use school devices and systems appropriately
• Communicate with pupils only through approved platforms
• Maintain professional boundaries online
• Protect personal and pupil data
• Follow the Staff Acceptable Use Agreement

Staff must NOT:
• Use personal phones to photograph pupils
• Add pupils on social media
• Message pupils through personal accounts
• Store pupil data on personal devices

Filtering and Monitoring
The school uses filtering and monitoring systems to identify potential risks online. Any alerts or concerns are reviewed by safeguarding staff.

Reporting Concerns
All concerns must be reported immediately to:

Designated Safeguarding Lead (DSL): Tina Clarke
Deputy DSL: Dani Rees / Lisa Solanki

If a child is in immediate danger, follow safeguarding procedures and contact emergency services if required.

REMEMBER - Online safety is safeguarding. If in doubt – report it.

Appendix G - Classroom Poster:

ONLINE SAFETY RULES

FISHERGATE PRIMARY SCHOOL

Don't Give Out Personal Information

Never share your:

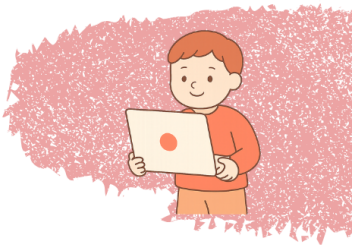
- full name
- address
- phone number
- passwords

Be Kind Online

Always use kind words and treat others with respect.

Tell an Adult if Something Feels Wrong

If something online makes you feel worried, upset or uncomfortable:
TELL A TRUSTED ADULT STRAIGHT AWAY!



Don't Talk to Strangers Online

Only communicate with people you know in real life

Ask for help

If something pops up or something happens you don't understand, ask an adult for help.

STOP – CLOSE – TELL

STOP using the device CLOSE the screen or app TELL a trusted adult