



Withycombe Raleigh Primary School

Online Safety Policy

Policy Reviewed and Ratified by Governors	
Date of next Review	

Key Personnel			
Role	Name	Email	Telephone
Designated Safeguarding Lead (DSL)	Michael Smith	msmith@wrpschool.org	01395 263397
Deputy DSL	Emma Jones	ejones@wrpschool.org	01395 263397
Deputy DSL	Sam Wheeler	swheeler@wrpschool.org	01395 263397
Headteacher	Emma Jones	ejones@wrpschool.org	01395 263397
Online Safety Lead	Stacey Williams	sjwilliams@wrpschool.org	01395 263397
Computing Lead			
Chair of Governors	Alison Longhorn	alonghorn@wrpschool.org	
Safeguarding Governor	Alison Longhorn	alonghorn@wrpschool.org	
Safeguarding Governor	Anna Slade	aslade@wrpschool.org	

Related Policies and Documents

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Staff Acceptable Use Agreement
- Pupil Acceptable Use Agreements
- Parent/Carer Online Safety Agreement
- RSHE Policy
- Computing Curriculum Policy
- Data Protection Policy
- Remote Learning Policy (where applicable)
- Equality Policy

Contents

1. Introduction and Rationale
2. Our Approach to Online Safety
3. Roles and Responsibilities
4. Filtering and Monitoring
5. Artificial Intelligence (AI)
6. Online Harms and Safeguarding Risks
7. Cyber Security
8. Mobile Phones and Personal Devices
9. Online Safety Education
10. Responding to Online Safety Incidents

Appendices:

- A. Staff Acceptable Use Agreement
- B. Pupil Acceptable Use Agreement
- C. Parent/Carer Online Safety Agreement
- D. Mobile Technology Agreement
- E. Online Safety Incident Response Flowchart
- F. Annual Online Safety, Filtering and Monitoring Review Record

Policy development, monitoring and review

This Online Safety Policy has been developed by the Online Safety Group including:

- Headteacher
- Designated Safeguarding Lead (DSL)
- Online Safety Lead (OSL)
- Staff members– including teachers/support staff/technical staff
- Governors
- Parents and carers
- Pupils

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development, Monitoring and Review

The implementation of this Online Safety Policy will be monitored by:	<i>DSL, OSL and Online Safety Governor</i>
The <i>governing body</i> will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>At Full Governors' meetings (at least termly)</i>

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>Annually or more frequently</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>Safeguarding Governors (Alison Longhorn / Anna Slade) Community Police IT provider: CTS Cornwall</i>

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents (recorded on cpoms)
- Filtering and monitoring logs
- Internal monitoring data for network activity
- Surveys/questionnaires of learners, parents and staff.

1. Introduction and Rationale

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Withycombe Raleigh C of E Primary School (WRPS) to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Technology provides significant opportunities for children's learning, creativity, communication and personal development. Digital technologies support teaching and learning across the curriculum and enable children to develop important skills needed for life beyond school.

However, the school recognises that children may also encounter risks when using technology, including:

- harmful or inappropriate content;
- inappropriate communication;
- cyberbullying;
- online exploitation;
- misinformation and fake information;
- privacy and data protection concerns;
- unhealthy online behaviours;
- risks associated with emerging technologies including artificial intelligence.

Online safety is therefore not solely a technical issue. It is a safeguarding responsibility shared by the whole school community.

At Withycombe Raleigh Primary School, online safety is embedded within our wider safeguarding culture and reflects our school expectations:

Be ready: Children are ready to learn how to use technology responsibly.

Be respectful: Children communicate positively and respectfully online.

Be safe: Children understand risks, know how to seek help and make safe choices.

The school recognises that effective online safety requires a combination of:

- education and awareness;
- appropriate filtering and monitoring;
- clear expectations and acceptable use agreements;
- staff training;
- effective safeguarding procedures;
- partnership with parents and carers.

2. Our Approach to Online Safety

Our aim is to ensure that all members of the Withycombe Raleigh community understand how to use technology safely, responsibly and respectfully.

We aim to ensure that:

- children develop the knowledge, skills and confidence to stay safe online;
- pupils understand how their online actions can affect themselves and others;
- children develop resilience and critical thinking when engaging with online content;
- staff understand their safeguarding responsibilities relating to technology;
- filtering and monitoring systems effectively support safe learning;
- online concerns are identified, recorded and responded to appropriately;
- parents and carers are supported in helping children stay safe online.

Online safety is taught and reinforced through:

Computing Curriculum

Children are taught:

- how to use technology safely;
- how to keep personal information private;
- how to recognise online risks;
- how to report concerns;
- how to behave responsibly online.

RSHE Curriculum

Children learn about:

- respectful relationships online;
- consent and boundaries;
- healthy use of technology;
- online communication;
- recognising unsafe situations.

Wider School Life

Online safety is reinforced through:

- assemblies;
- safeguarding education;
- pastoral support;
- pupil voice activities;
- themed events such as Safer Internet Day;
- conversations with parents and carers.

3. Roles and Responsibilities

Effective online safety depends upon everyone in the school community understanding their role and responsibility. Online safety is a safeguarding responsibility and should be embedded within the culture of Withycombe Raleigh Primary School.

Governing Body

The Governing Body will:

- ensure that online safety is considered as part of the school's safeguarding responsibilities;
- ensure that appropriate online safety policies and procedures are in place;
- receive regular updates regarding online safety, filtering and monitoring arrangements;
- ensure that the effectiveness of filtering and monitoring systems is reviewed regularly;
- provide appropriate challenge and support to school leaders;
- ensure that staff receive appropriate training and updates;
- review this policy annually or sooner where there are significant changes to guidance, technology or school practice.

Governors will receive assurance that the school is meeting its responsibilities in relation to:

- Keeping Children Safe in Education (KCSIE);
- Department for Education filtering and monitoring expectations;
- Safeguarding responsibilities relating to technology.

Headteacher

The Headteacher will:

- ensure online safety remains a safeguarding priority;
- ensure appropriate systems, policies and procedures are implemented;
- ensure staff understand their responsibilities relating to online safety;
- ensure appropriate training is provided for staff;
- ensure concerns are managed effectively through safeguarding procedures;
- work with the DSL and technical providers to review online safety arrangements;
- ensure governors receive appropriate information and assurance.

Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for safeguarding concerns relating to online safety.

The DSL will:

- lead the school's online safety safeguarding practice;
- ensure online safety forms part of the school's safeguarding culture;
- oversee responses to online safeguarding concerns;
- ensure concerns are recorded appropriately on CPOMS;
- determine whether online incidents represent safeguarding concerns;
- liaise with parents, carers and external agencies where appropriate;
- work with IT providers regarding filtering and monitoring concerns;
- review filtering and monitoring reports and concerns;
- ensure staff understand reporting procedures;
- identify emerging online risks and update practice accordingly;
- ensure online safety education is embedded across the curriculum.

Where appropriate, the DSL will consider whether concerns require referral to:

- the Devon Multi-Agency Safeguarding Hub (MASH);
- the Police;
- other relevant safeguarding partners.

Computing Subject Leader

The Computing Subject Leader will:

- ensure online safety education is effectively planned and delivered;
- ensure curriculum content reflects current online risks and technologies;
- support staff confidence in teaching online safety;
- identify opportunities for pupils to develop digital literacy;
- work with the DSL to ensure curriculum content reflects safeguarding priorities.

All Staff

All members of staff have a responsibility to promote and maintain online safety.

Staff must:

- model safe, respectful and responsible technology use;
- follow the Staff Acceptable Use Agreement;
- report concerns immediately;
- record safeguarding concerns appropriately;
- understand that online concerns may represent wider safeguarding issues;
- maintain professional boundaries when using technology;
- protect confidential information;
- use approved systems and platforms.

Staff should recognise that children may disclose online concerns in the same way they may disclose other safeguarding concerns.

Pupils

Pupils are expected to:

- follow the school's online safety expectations;
- use technology respectfully and responsibly;
- protect their own and others' personal information;
- report anything that makes them feel worried, uncomfortable or unsafe;
- follow the school rules: **Be ready, be respectful, be safe.**

Parents and Carers

Parents and carers play an important role in supporting children's online safety.

The school will:

- provide information and guidance about online risks;
- share relevant online safety resources;
- encourage positive conversations about technology at home;
- support parents in understanding emerging risks.

Parents and carers are encouraged to:

- talk regularly with children about their online experiences;
- understand the platforms and games children use;
- encourage safe and respectful online behaviour;
- report concerns to school where appropriate.

4. Filtering and Monitoring

Withycombe Raleigh Primary School recognises that effective filtering and monitoring arrangements are an important part of safeguarding children online.

The school uses **RM SafetyNet** to support filtering and monitoring of online activity.

Filtering and monitoring systems help reduce the likelihood of children accessing harmful or inappropriate content; however, the school recognises that technology alone cannot keep children safe. Effective online safety requires:

- education;
- supervision;
- professional judgement;
- clear expectations;
- appropriate safeguarding responses.

Filtering

The school will ensure that filtering systems:

- are appropriate for the age and needs of pupils;
- are regularly reviewed;
- support safe access to educational resources;
- block inappropriate and harmful content;
- are reviewed when new risks emerge.

The school recognises that no filtering system can guarantee that all harmful content will be blocked. Staff must therefore remain vigilant and report concerns.

Monitoring

The school will monitor online activity to help identify:

- attempts to access inappropriate content;
- safeguarding concerns;
- misuse of school systems;
- emerging online risks.

Monitoring information may be reviewed by appropriate staff, including:

- Headteacher;
- DSL;
- members of the safeguarding team;
- approved technical support staff.

Filtering and Monitoring Review Process

The DSL, Headteacher and technical support staff will work together to review:

- filtering effectiveness;
- monitoring alerts;
- blocked websites and categories;
- false positives;
- emerging online risks;
- pupil and staff concerns;
- any incidents involving inappropriate access.

Findings will inform:

- safeguarding practice;
- staff training;
- curriculum development;
- governor assurance.

Responding to Filtering and Monitoring Concerns

Where a concern is identified:

1. The concern will be reviewed.
2. The context and risk will be considered.
3. Appropriate action will be taken.
4. Safeguarding concerns will be recorded on CPOMS.
5. Further action will be taken where required.

This may include:

- discussion with pupils;
- parent/carers communication;
- additional teaching or support;
- behaviour consequences;
- safeguarding referral.

5. Artificial Intelligence (AI)

Withycombe Raleigh Primary School recognises that artificial intelligence is developing rapidly and will increasingly influence children's education and future lives.

AI provides opportunities to:

- support creativity;
- develop ideas;
- improve accessibility;
- support teaching and learning.

However, AI also presents risks which the school must manage.

Potential Risks of AI

These include:

- inaccurate or misleading information;
- inappropriate content generation;
- loss of privacy;
- misuse of AI-generated images, audio or video;
- creation of harmful or misleading content;
- over-reliance on technology rather than critical thinking.

Staff Use of AI

Staff may use AI tools where this supports their professional work and where use is consistent with school expectations.

Staff must:

- use professional judgement;
- check the accuracy of AI-generated information;
- ensure resources are appropriate for children;
- maintain confidentiality.

Staff must **not** enter:

- pupil personal information;
- safeguarding information;
- family information;
- confidential school data;

into AI tools unless the platform has been approved by the school.

Pupils and AI

Pupils will be taught to:

- question the accuracy of information;
- understand that AI-generated content may not be reliable;
- use technology responsibly;
- respect privacy;
- understand the impact of creating and sharing digital content.

6. Online Harms and Safeguarding Risks

Withycombe Raleigh Primary School recognises that children may experience a range of risks when using digital technologies. These risks are constantly evolving, and the school remains committed to educating pupils, supporting families and responding effectively to concerns.

The school uses the recognised **four categories of online risk**:

- **Content**
- **Contact**
- **Conduct**
- **Consumer**

Content Risks

Content risks relate to children being exposed to material which may be harmful, inappropriate or unsuitable.

Examples may include:

- violent or hateful content;
- pornography or sexualised material;
- misinformation and fake news;
- content promoting unsafe behaviours;
- harmful online challenges;
- extremist or radicalising content;
- inappropriate advertising;
- content designed to manipulate or exploit children.

The school supports pupils to:

- develop critical thinking skills;
- question whether online information is reliable;
- understand that not everything online is true or safe;
- report content that makes them feel worried or uncomfortable.

Contact Risks

Contact risks relate to children communicating with others online.

Examples may include:

- inappropriate messages;
- unwanted contact;
- grooming;
- online exploitation;
- manipulation or coercion;
- harmful online relationships;
- adults pretending to be someone else online.

The school teaches children:

- not everyone online is who they claim to be;
- they should never keep online secrets that make them feel uncomfortable;
- they should seek help from a trusted adult if something worries them;
- safe and respectful communication is expected online.

Conduct Risks

Conduct risks relate to how children behave online and how their actions may affect themselves or others.

Examples may include:

- cyberbullying;
- online arguments;
- harassment;
- sharing harmful content;
- creating or sharing inappropriate material;
- misuse of school technology;
- damaging someone's reputation online.

The school promotes our values: **Generosity, Respect, Agape, Courage and Empathy**

Children are reminded that these values apply equally online and offline.

Consumer Risks

Consumer risks relate to children interacting with online services, advertising and commercial activity.

Examples may include:

- scams;
- inappropriate advertising;
- pressure to purchase items;
- online gambling-style features;
- misuse of personal information;
- unsafe online purchases.

Pupils are taught to:

- protect personal information;
- recognise persuasive online techniques;
- ask for adult support when unsure.

Emerging Online Risks

The school recognises that online risks continue to change. Emerging areas include:

- artificial intelligence;
- deepfakes and manipulated media;
- livestreaming;
- gaming platforms;
- online communities;
- social media trends;
- inappropriate use of digital devices.

The DSL and Computing Subject Leader will review emerging risks and ensure school practice remains appropriate.

7. Cyber Security

Withycombe Raleigh Primary School recognises that cyber security is an important part of safeguarding. Protecting school systems, information and personal data helps protect children, families and staff.

All staff must follow school expectations regarding:

- passwords;
- information security;
- data protection;
- use of devices;
- access to school systems.

Staff Responsibilities

Staff must:

- use secure passwords;
- never share passwords with others;
- lock devices when unattended;
- only access information necessary for their role;
- report suspicious emails or activity;
- follow data protection procedures;
- use approved software and systems.

Cyber Security Incidents

Concerns may include:

- phishing emails;
- suspicious links or attachments;
- loss of devices;
- unauthorised access;
- accidental sharing of information;
- malware or security alerts.

Concerns should be reported immediately to the appropriate member of staff.

Where a concern involves personal data, the school will follow its Data Protection procedures.

8. Mobile Phones and Personal Devices

Withycombe Raleigh Primary School recognises that mobile phones and personal devices are part of children's lives outside school.

The school aims to ensure that technology supports children's learning, wellbeing and safety.

Pupil Expectations

Children must follow school expectations regarding:

- mobile phones;
- smart watches;
- personal devices;
- cameras and recording equipment.

Personal devices should not:

- disrupt learning;
- be used to record others without permission;
- be used inappropriately;
- create safeguarding concerns.

Staff Personal Devices

Staff must ensure personal devices are used appropriately.

Staff should:

- maintain professional boundaries;
- avoid storing pupil information on personal devices;
- avoid taking photographs of pupils using personal devices;
- follow school expectations regarding communication.

Visitors and Volunteers

Visitors and volunteers should follow school expectations regarding mobile phones and photography.

The school will ensure that:

- photographs and videos of children are only taken using approved systems;
- parental consent arrangements are followed;
- safeguarding expectations are communicated clearly for example photos and videos should not be shared on social media or posted in a way that allows broader public viewing.

9. Online Safety Education

At Withycombe Raleigh Primary School, online safety education is embedded throughout the curriculum and wider school life.

Children are taught that being safe online is part of being a responsible member of the school community.

Computing Curriculum

Through Computing, pupils learn:

- how to use technology safely;
- how to keep information private;
- how to communicate responsibly;
- how to recognise online risks;
- how to report concerns (about themselves and their peers);
- how to evaluate online information.

RSHE Curriculum

Through RSHE, pupils learn:

- respectful relationships online;
- consent and boundaries;
- kindness and empathy online;
- managing online friendships;
- recognising unsafe situations;
- seeking support.

Safeguarding Education

Online safety is reinforced through:

- assemblies;
- themed weeks and events;
- pastoral conversations;
- targeted support;
- pupil voice activities.

The school recognises that different children may require different levels of support depending on:

- age;
- maturity;
- additional needs;
- online experiences;
- vulnerability factors.

10. Responding to Online Safety Incidents

All members of the school community are encouraged to report online safety concerns.

Children should know:

“If something happens online that makes you feel worried, uncomfortable or unsafe, tell a trusted adult.”

Examples of Online Safety Concerns

Concerns may include:

- cyberbullying;
- inappropriate messages;
- harmful content;
- online exploitation;
- grooming concerns;
- sharing inappropriate images;
- misuse of school technology;
- online threats;
- identity or privacy concerns.

Reporting Process

When a concern is raised:

Step 1 – Listen and Respond

Staff should:

- listen carefully;
- reassure the child;
- avoid judgement;
- gather appropriate information;
- avoid promising secrecy.

Step 2 – Record

Where appropriate, concerns should be recorded on **CPOMS** in line with safeguarding procedures.

Records should include:

- what happened;
- who was involved;
- when it happened;
- actions taken;
- decisions made.

Step 3 – Assess Risk

The DSL will consider:

- whether the concern is a safeguarding matter;
- whether further information is required;
- whether parents/carers should be informed;
- whether external agencies need to be involved.

Step 4 – Take Appropriate Action

Actions may include:

- support for the child;
- restorative conversations;
- curriculum support;
- behaviour responses;
- parent/carer communication;
- referral to external agencies.

Staff Training and Awareness

All staff will receive appropriate online safety training to ensure they understand:

- current online risks;
- reporting procedures;
- filtering and monitoring arrangements;
- acceptable technology use;
- safeguarding responsibilities.

Online safety updates will form part of:

- safeguarding updates;
- staff briefings / meetings;
- professional development.

Partnership with Parents and the Wider Community

The school recognises that children's online lives continue beyond the school day.

We will work with parents and carers by:

- sharing online safety guidance;
- signposting trusted resources;
- encouraging open conversations about technology;
- providing support when concerns arise.

Appendices

Appendix A:

Staff Acceptable Use Agreement; Safe and Responsible Use of Technology

Purpose: Technology is an essential part of teaching, learning, communication and safeguarding at Withycombe Raleigh Primary School.

Staff are expected to use technology in a way that:

- protects children and families;
- maintains professional boundaries;
- protects confidential information;
- models safe and respectful online behaviour;
- supports learning and school improvement.

This agreement should be read alongside:

- Online Safety Policy;
- Child Protection and Safeguarding Policy;
- Staff Code of Conduct;
- Data Protection Policy;
- Whistleblowing Policy.

1. Staff Use of School Technology

Staff CAN:

- ✓ Use school devices and approved systems to support teaching, learning and professional responsibilities.
- ✓ Access appropriate educational websites, resources and online platforms.
- ✓ Use digital tools to improve planning, assessment, communication and pupil outcomes.
- ✓ Use approved cloud systems and school platforms for storing and sharing information.
- ✓ Use technology to support accessibility and inclusion for pupils.
- ✓ Use approved artificial intelligence tools where this supports professional practice and follows school guidance.

Staff MUST:

- ✓ Use professional judgement when accessing online content.
- ✓ Ensure resources used with pupils are age appropriate and suitable.

- ✓ Check websites, videos and digital resources before sharing with children.
- ✓ Report inappropriate content accessed accidentally.
- ✓ Keep devices secure and protected.
- ✓ Log out of systems when finished.
- ✓ Follow school procedures for reporting online safety concerns.

Personal devices must not be used in classrooms, pupil areas, toilets, changing areas or during supervision of pupils, unless there is an exceptional circumstance and explicit authorisation has been given by the Headteacher or the Designated Safeguarding Lead (DSL).

Staff MUST NOT:

- ✗ Use school technology to access, create, share or store inappropriate material.
- ✗ Access content that could reasonably be considered offensive, harmful, illegal or unsuitable for children.
- ✗ Circumvent school filtering systems or attempt to bypass security controls.
- ✗ Download unauthorised software, applications or browser extensions.
- ✗ Connect unknown devices or storage equipment without approval.
- ✗ Use school systems for personal business or activities that could compromise security.

2. Professional Online Communication

Staff must remember that online communication is part of their professional role.

Staff CAN:

- ✓ Communicate with parents and carers using approved school systems.
- ✓ Use approved platforms for teaching, learning and communication.
- ✓ Share information with colleagues through appropriate professional channels.
- ✓ Use technology to celebrate pupil achievements in line with school procedures.

Staff MUST:

- ✓ Maintain professional boundaries at all times.
- ✓ Use school email accounts and approved communication systems.
- ✓ Ensure messages are professional, respectful and appropriate.
- ✓ Consider that digital communication may be stored, forwarded or shared.
- ✓ Follow safeguarding procedures if a pupil communicates something concerning online.

Staff MUST NOT:

- X** Communicate with pupils using personal email accounts, personal messaging apps or private social media accounts.
- X** Accept pupil friend/follow requests on personal social media accounts.
- X** Message pupils privately through social media platforms.
- X** Share personal information with pupils.
- X** Give pupils personal contact details unless specifically authorised.
- X** Delete safeguarding-related messages or evidence before advice from the DSL.

3. Social Media

Staff should recognise that personal online activity can affect professional reputation.

Staff CAN:

- ✓ Maintain personal social media accounts.
- ✓ Express personal opinions appropriately and responsibly.

Staff MUST:

- ✓ Ensure privacy settings are appropriately managed.
- ✓ Consider the professional impact of online posts.
- ✓ Avoid posting anything that could damage confidence in themselves, colleagues or the school.
- ✓ Ensure they do not identify themselves as speaking on behalf of the school unless authorised.

Staff MUST NOT:

- X** Post photographs, videos or information about pupils on personal accounts.
- X** Discuss pupils, families or safeguarding matters online.
- X** Make comments that could undermine professional relationships.
- X** Share confidential school information.
- X** Engage in online arguments or inappropriate exchanges linked to the school.

4. Photographs, Videos and Recording

Staff CAN:

- ✓ Take photographs and videos of pupils using approved school devices and systems.
- ✓ Use images for approved educational purposes where consent procedures have been followed.
- ✓ Record learning activities where this supports assessment or curriculum development.

Staff MUST:

- ✓ Follow parental consent arrangements.
- ✓ Store images securely.
- ✓ Use school-approved platforms for sharing.
- ✓ Delete images when they are no longer required.

Staff MUST NOT:

- ✗ Use personal mobile phones or personal cameras to photograph or record pupils.
- ✗ Share pupil images through personal accounts.
- ✗ Store pupil images on personal devices.
- ✗ Take images of children without an appropriate educational or safeguarding purpose.
- ✗ Wear Meta Glasses on the school site due to their covert nature.

5. Artificial Intelligence (AI)

Staff CAN:

- ✓ Use approved AI tools to support planning, administration and professional development.
- ✓ Use AI to generate ideas, resources or prompts.
- ✓ Use AI to improve efficiency where appropriate.

Staff MUST:

- ✓ Check AI-generated content for accuracy.
- ✓ Ensure resources are appropriate for pupils.
- ✓ Maintain professional judgement.
- ✓ Consider bias, accuracy and suitability.

Staff MUST NOT:

- X** Enter confidential pupil information into AI tools.
- X** Enter safeguarding records or CPOMS information into AI tools.
- X** Enter personal details about children, families or staff.
- X** Use AI to make decisions about pupils without professional oversight.
- X** Create or share AI-generated content that could harm, embarrass or misrepresent others.

6. Passwords and Cyber Security

Staff MUST:

- ✓ Use strong passwords.
- ✓ Keep passwords confidential.
- ✓ Use multi-factor authentication where available.
- ✓ Lock screens when leaving devices unattended.
- ✓ Report suspected phishing emails.
- ✓ Report lost or stolen devices immediately.

Staff MUST NOT:

- X** Share passwords.
- X** Leave confidential information visible.
- X** Use another person's account.
- X** Store sensitive information on personal devices.
- X** Click suspicious links or attachments.

7. Use of Personal Devices

Staff CAN:

- ✓ Use personal devices appropriately during non-contact time.
- ✓ Use personal devices in designated staff areas agreed by the school (for example, the staff room or meeting room).
- ✓ Use personal devices for approved personal purposes.

Staff MUST NOT:

- X** Use personal devices to access or store pupil information.
- X** Photograph or record pupils.
- X** Use personal messaging apps to communicate with pupils.
- X** Allow pupils to use personal devices.

8. Reporting Concerns

Concerns About Pupil Conduct Online or the Use of Technology

Staff must report:

- inappropriate content;
- suspicious messages;
- cyber security concerns;
- online bullying;
- concerns about pupil online activity;
- misuse of technology;
- breaches of this agreement.

Concerns should be reported to:

- the DSL / Headteacher for safeguarding concerns;
- the appropriate technical support route for IT concerns.

Safeguarding concerns should be recorded through **CPOMS**.

Reporting Concerns About Staff Conduct Online or the Use of Technology

Withycombe Raleigh Primary School is committed to maintaining a culture of safeguarding, openness and professional accountability. Concerns about the online conduct of staff, volunteers, governors, contractors or any adult working in the school must be taken seriously and reported appropriately.

Technology-related concerns may include, but are not limited to:

- inappropriate online communication with pupils, parents / carers and other staff members;
- breaches of professional boundaries;
- inappropriate use of social media;
- use of personal devices in breach of school policy;
- taking or storing images of pupils inappropriately;
- accessing inappropriate online content on school equipment;
- misuse of school technology systems;
- inappropriate use of artificial intelligence (AI) tools;
- behaviour that may indicate a safeguarding risk.

Reporting concerns

All staff have a responsibility to report concerns about the conduct of another adult where that behaviour may:

- be inconsistent with the Staff Code of Conduct;
- breach the Online Safety Policy;
- create a safeguarding risk;
- undermine professional standards; or
- damage confidence in the school's safeguarding culture.

Concerns should be reported promptly to the Headteacher or Deputy Head. Where the concern relates to the Headteacher, it should be reported to the Chair of Governors.

Low-level concerns: Concerns that do not meet the threshold for an allegation may still be significant. These should be reported in accordance with the school's Low-Level Concerns Policy.

Examples may include:

- inappropriate or excessive personal use of technology around pupils;
- concerning social media interactions;
- poor judgement in online communication;
- failure to follow acceptable use expectations;
- inappropriate use of personal devices;
- behaviour that gives rise to a sense of unease, discomfort or doubt about professional conduct.

The purpose of reporting low-level concerns is to:

- identify patterns of behaviour;
- promote early intervention;
- protect pupils and to support staff;
- maintain a culture of transparency and safeguarding.

Staff should never assume that someone else will report a concern. All reports will be considered fairly, confidentially and in accordance with the school's safeguarding, disciplinary and low-level concerns procedures.

Staff Declaration: I confirm that I have read and understood this agreement and agree to follow the expectations for safe and responsible technology use.

Name: _____

Signature: _____

Date: _____

Appendix B

Pupil Acceptable Use Agreement

EYFS and Key Stage 1 Version

At Withycombe Raleigh Primary School, we use technology to help us learn.

We follow our school rules: **Be ready. Be respectful. Be safe.**

When I use technology, I will:

- ☐ Ask an adult if I need help.
- ☐ Use devices carefully.
- ☐ Be kind and respectful online.
- ☐ Tell an adult if something worries me.
- ☐ Keep my passwords private.
- ☐ Only use websites and apps my teacher says are safe.
- ☐ Treat other people's information and work with respect.

I understand:

- I should not look for things online that are unsafe or unkind.
- I should tell an adult if something makes me feel worried.
- My actions online can affect other people.

Name: _____

Class: _____

Date: _____

Key Stage 2 Version

Using Technology Safely

I agree that I will:

- ☐ Use technology responsibly and respectfully.
- ☐ Follow instructions from staff.
- ☐ Keep my passwords private.
- ☐ Respect other people's privacy.
- ☐ Think carefully before posting, sharing or sending anything online.
- ☐ Report anything that makes me feel uncomfortable or unsafe.
- ☐ Use school technology only for appropriate purposes.
- ☐ Treat others online with kindness and respect.

I understand that:

- Everything I do online leaves a digital footprint.
- Online behaviour should reflect our school values.
- Sharing harmful or unkind content can hurt others.
- I should seek help from a trusted adult if I have concerns.

Name: _____

Signature: _____

Class: _____

Date: _____

Appendix C

Parent/Carer Online Safety Agreement

Working Together to Keep Children Safe Online

At Withycombe Raleigh Primary School, we recognise that children's online experiences continue beyond the school day.

Parents and carers play an essential role in helping children develop safe and healthy digital habits.

We ask parents and carers to:

- ☐ Talk regularly with their child about their online experiences.
- ☐ Encourage children to tell a trusted adult if something worries them.
- ☐ Understand the apps, games and websites their child uses.
- ☐ Support safe and respectful online behaviour.
- ☐ Check privacy settings and age requirements for online platforms.
- ☐ Encourage children not to share personal information online.
- ☐ Report concerns to school where appropriate.

We encourage families to:

- create clear expectations around screen use, including age-related content;
- model respectful digital behaviour;
- discuss online friendships and communication;
- help children understand that not everything online is true;
- seek support if they have concerns.

Agreement

I understand that keeping children safe online is a shared responsibility between home and school.

Parent/Carer name: _____

Signature: _____

Date: _____

Appendix D

Mobile Technology Agreement

Pupil Mobile Phones and Personal Devices

Withycombe Raleigh Primary School does not permit pupils to use mobile phones, smart watches or other personal mobile technology during the school day.

Pupils who need to bring a mobile phone to school (for example, because they travel independently to or from school) may do so only with parental agreement and the permission of the school.

School expectations

- Any mobile phone brought onto the school site **must be switched off before entering the school grounds.**
- The phone **must be handed in to the school office or to the class teacher immediately on arrival.**
- The phone will be stored securely during the school day.
- The phone will be returned to the pupil at the end of the school day.
- Pupils must not access or use their mobile phone at any point during the school day unless authorised by the Headteacher or the Designated Safeguarding Lead (DSL).

Smart watches and other connected devices

Smart watches with communication, internet or recording functions should not be worn during the school day. Where such a device is brought to school, it must be handed in with the pupil's mobile phone.

Unauthorised devices

If a pupil is found using a mobile phone or other personal mobile technology during the school day, the device will be confiscated and retained securely. Parents or carers will be required to collect the device and the incident may be dealt with in accordance with the school's Behaviour Policy and Online Safety Policy.

These arrangements are intended to protect pupils' learning, wellbeing, privacy and safeguarding and to ensure a safe and focused learning environment for all children.

Appendix E

Online Safety Incident Response Flowchart - Online Safety Concern Raised

1. Immediate Response

Staff member:

- listens;
- reassures the child, avoiding judgement;
- gathers information;
- does not promise confidentiality.

2. Record Concern

Record on CPOMS where appropriate.

Include:

- what happened;
- who was involved;
- date/time;
- actions taken.

3. DSL Review

DSL considers:

- safeguarding risk including level of harm;
- support required;
- whether parents/carers should be contacted;
- outcomes and learning points / next steps.

4. Action

Possible actions:

- pupil support;
- education and advice;
- behaviour response / consequence;
- parent/carer involvement;
- external referral.

Appendix F

Annual Online Safety, Filtering and Monitoring Review Record

(DSL, Headteacher, Online Safety Lead, Online Safety Group and Online Safety Governor)

Annual Review Record

Date of review: _____

Completed by: _____

Filtering System: RM SafetyNet

Review period: _____

Reported to: Online Safety Group / Governing Body

Online Safety Governor: _____

Purpose of Review

This annual review ensures that the school's online safety, filtering and monitoring arrangements remain effective in protecting children from harmful online content while enabling access to appropriate educational resources.

The review is completed by the DSL, Headteacher, Online Safety Lead and Online Safety Group. The Online Safety Governor provides challenge and assurance on behalf of the Governing Body.

The review supports the school's safeguarding responsibilities, the DfE Filtering and Monitoring Standards, and the ongoing development of online safety education and practice.

1. Filtering Review

Review Area	Evidence / Notes / Actions
Is filtering appropriate for the age, needs and curriculum requirements of pupils?	
Are harmful categories and inappropriate content blocked effectively?	
Are filtering arrangements aligned with the DfE Filtering and Monitoring Standards?	
Are pupils and staff able to access appropriate educational resources without unnecessary restriction?	
Are filtering change requests considered, recorded and reviewed appropriately?	
Are filtering incidents and concerns recorded and followed up through safeguarding procedures where required?	
Are staff aware of how to report concerns or request filtering reviews?	

2. Monitoring Review

The Online Safety Group will support the DSL and Online Safety Lead by reviewing available monitoring information, including:

- monitoring alerts and reports;
- blocked searches and attempted access to inappropriate content;
- trends or repeated concerns;
- emerging online risks affecting children;
- concerns raised by pupils, staff, parents/carers or external agencies;
- incidents recorded through safeguarding systems.

Monitoring Review Area	Evidence / Notes / Actions
Are monitoring alerts reviewed regularly by appropriate staff?	
Are safeguarding concerns identified through monitoring followed up appropriately?	
Are repeated incidents or patterns identified and addressed?	
Are emerging online risks reflected in online safety education and staff training?	

Are pupils given opportunities to contribute to understanding online risks and improving online safety provision?

3. Online Safety Group Responsibilities

The Online Safety Group supports the ongoing review and improvement of online safety provision by:

- ☐ Reviewing the effectiveness of filtering and monitoring systems.
- ☐ Considering reports and trends from filtering and monitoring activity.
- ☐ Reviewing the Online Safety Policy and associated procedures.
- ☐ Monitoring the impact of online safety education across the school.
- ☐ Ensuring online safety teaching is relevant, age-appropriate, progressive and responsive to emerging risks.
- ☐ Consulting with pupils, staff and parents/carers about online safety provision.
- ☐ Encouraging pupil voice and contributions to understanding emerging online risks.
- ☐ Considering improvements identified through the SWGfL 360-degree safe self-review tool.
- ☐ Reporting significant findings, risks and recommended actions to the Headteacher and Governing Body.

4. Governor Online Safety Assurance Checklist

Policy and Leadership

- ☐ Online Safety Policy reviewed annually.
- ☐ Online safety is included within safeguarding oversight.
- ☐ Governors receive appropriate updates regarding online safety, including through Full Governing Body meetings.
- ☐ Staff online safety training is current and appropriate.
- ☐ The school has clear leadership responsibility for online safety.

Filtering and Monitoring

- ☐ Filtering and monitoring arrangements are effective.
- ☐ RM SafetyNet arrangements are reviewed regularly.
- ☐ Concerns, alerts and incidents are monitored and acted upon appropriately.
- ☐ Governors receive assurance regarding the effectiveness of filtering and monitoring systems.
- ☐ The school has a clear process for reporting and responding to online safety concerns.

Curriculum and Pupil Education

- ☐ Online safety is taught through Computing.
- ☐ Online safety is reinforced through RSHE and wider curriculum opportunities.
- ☐ Pupils understand how to report concerns and seek help.
- ☐ Digital citizenship, responsible behaviour and critical thinking online are promoted.
- ☐ Online safety education reflects current and emerging risks.

Safeguarding

- ☐ Online safety concerns are recorded appropriately through safeguarding systems.
- ☐ The DSL reviews emerging online risks and trends.
- ☐ Appropriate safeguarding referrals are made where required.
- ☐ Vulnerable pupils receive appropriate support and consideration regarding online risks.

Parent and Community Engagement

- ☐ Parents/carers receive online safety guidance and support.
- ☐ The school signposts families to trusted online safety resources.
- ☐ Parents/carers know how to raise online safety concerns with the school.
- ☐ The school works with the wider community to promote safe and responsible online behaviour.

Actions and Improvements Identified

Action Required	Person Responsible	Timescale	Completed
-----------------	--------------------	-----------	-----------