SKERTON ST LUKE'S CE VA PRIMARY SCHOOL

**Live, Learn, Thrive; Love God, Love Each other.**

POLICY FOR

# ONLINE SAFETY

Reviewed: Spring 2026
Review Due: Spring 2028

## School Christian Values

Generosity, compassion, courage, forgiveness, friendship, respect,

Thankfulness, trust, perseverance, justice, service and truthfulness.

## Our school values are:

wisdom respect perseverance aspiration service justice

## Bible Reference

Luke 10: 27 'Love your neighbour as yourself'

## Policy References

This policy is written with reference to the following school policies:

- Curriculum Policy,
- Learning and Teaching Policy,
- Marking Policy,
- Safeguarding & Child Protection Policy,
- Single Equalities Policy.
- Health and Safety

Most of these policies are available on the school website. In addition, copies of the following policies are available, on request, from the school office.

**Contents:**



**Introduction**

At Skerton St Luke's CE Primary School, our Christian vision—Live, Learn, Thrive; Love God, Love Each Other—guides our safeguarding practice. We believe every child is valued, protected and supported to flourish.

Technology is central to learning and daily life. While it offers many benefits, it also presents risks. We are committed to teaching pupils to use digital tools safely, responsibly and with discernment, preparing them for lifelong learning and future employment.

Pupils engage with a wide range of online technologies, including websites, apps, messaging tools, social media, streaming services, online gaming, smart devices and emerging AI systems. This rapidly changing landscape requires clear guidance and strong digital literacy.

As a school, we recognise our responsibility to educate pupils—and support families—so they understand online risks and develop the knowledge, behaviours and critical thinking needed to stay safe and act legally both in school and beyond.

## Intent:

- **Foster curiosity** by providing progressive access to a wide range of digital information and contexts.
- **Develop critical thinking** to solve problems in the digital world truthfully and responsibly.
- **Build confidence** in using a variety of digital tools in school and beyond.
- **Promote safe and respectful connection** through hardware, software and media grounded in Christian values.
- **Teach responsible online behaviour**, helping pupils understand the impact of their actions and recognise respectful conduct.
- **Enable safe navigation** of the online world with perseverance, wise judgement and awareness across all devices, apps and platforms.

## Key Roles and Responsibilities:

### Computing Subject Leader

- **Promote online safety** across all technology-based learning.
- **Provide staff training** and share regular updates on online safety.
- **Attend external training** and implement guidance.
- **Maintain and update computing policies**.
- **Support curriculum and resource implementation**.
- **Oversee filtered internet access** appropriate to pupils' age and needs.

### Designated Safeguarding Lead (DSL)

- **Provide online safety training** and regular updates.
- **Attend external safeguarding training**.

- **Lead responses to online safety concerns** with the Safeguarding Team.

**Governors**

- **Champion online safety** across the school.
- **Monitor implementation** of curriculum, software, hardware and policies.
- **Ensure a designated computing lead** is in place.

**Staff**

- **Receive online safety training** at induction and through ongoing CPD.
- **Promote and embed online safety** in all technology-based teaching.
- **Monitor pupil technology use** and deliver a broad, balanced curriculum.
- **Report concerns** to the Safeguarding Team and log on CPOMS.
- **Inform parents of individual concerns** as advised by safeguarding staff.
- **Follow copyright requirements** for classroom and published materials.
- **Communicate professionally with external agencies**.

**Parents**

- **Access up-to-date online safety resources** including weekly Wake Up Wednesday links and webinars and parent support sessions through Coram/Scarf Education.
- **Support the school's Online Safety Policy**.
- **Report concerns** to school staff.
- **Stay informed** through newsletters, the website, Parent App and assemblies/ support sessions.

**Pupils**

- **Use technology appropriately** as instructed by staff.
- **Report online safety concerns** to a trusted adult.
- **Participate in school parliament** discussions on online safety.
- **Support device care** through KS2 Gadget Guardians and Charging Champions.

## Teaching Online Safety

Skerton St Luke's CE Primary School teaches online safety through the Teach Computing curriculum, informed by **KCSIE, Education for a Connected World, and National Curriculum** objectives. Christian values—respect, courage, forgiveness and compassion—are embedded throughout to support wise and loving behaviour online.

Online safety is taught through **age-appropriate units from EYFS to Year 6**, with additional teaching when issues arise. Learning is integrated across Computing, PSHE and wider curriculum areas to prepare pupils for an ever-changing digital world.

**Pupils Are Taught To**

- **Seek help** when something online worries them and know who to report to (trusted adult, Childline, CEOP, NSPCC, KIDSAFE, CORAM/SCARF education).
- **Understand and respond to online bullying appropriately.**
- **Use the internet critically,** including evaluating information for accuracy.
- **Communicate safely** and avoid sharing personal information**.**

# Monitoring, Filtering and Management

Skerton St Luke's CE Primary School maintains robust filtering and monitoring systems to safeguard pupils online while supporting effective teaching and learning. These systems uphold safety, dignity and responsible stewardship.

## Filtering

- **Filtering systems** limit exposure to harmful or inappropriate content, including on remote devices.
- The school uses **Net Sweeper**, with daily virus-protection updates overseen by the school technician.
- Decisions to block or unblock content are made jointly by the **Headteacher**, **Computing Lead**, **DSLs**, and **Technician**, considering educational context.
- Filtering does **not** unreasonably restrict learning or prevent pupils from developing risk-assessment skills.
- Reviews cover school-owned devices, all site areas and all user groups. Checks are logged with date, staff member and actions taken.

## Monitoring

Monitoring ensures pupils' online activity is supervised and concerns are identified promptly.

1. **Physical Monitoring**
    - Pupils are supervised when using internet-enabled devices.
    - Devices are used only for teacher-directed educational purposes.
    - Devices are signed in and out using an in-school log – overseen by the Computing Lead.
    - Classes keep a class list to assign numbered devices to each child to support monitoring.
2. **Internet and Web Access Monitoring**
    - Daily updates, content checks and regular reviews of blocked sites are carried out by the monitoring team.
3. **Active Monitoring**
    - Net Sweeper sends automatic alerts to DSLs with details of the concern.
    - DSLs follow the **Safeguarding Policy**, record concerns on CPOMS and take appropriate action.

Any online safety concern must be reported immediately to a DSL and logged on CPOMS.

# Internet Access and Device Management

- KS2 pupils use numbered iPads or individual logins; teachers maintain usage logs within classes and class staff to sign in/out devices on the whole-school log sheet – overseen by Computing Leader.
- EYFS–KS1 pupils use supervised class logins and designated apps.
- Staff and pupils must not share passwords.
- Security strategies are reviewed regularly by senior leaders and the Computing Lead.
- The school works with the **IT Technician**, **LA**, **DfE**, and **Net Sweeper** to maintain and improve systems.
- Any unsuitable site must be reported to the Class Teacher, Computing Lead, Technician, Headteacher or DSL and then logged on CPOMS.

The technician and administration team ensure filtering methods remain appropriate and effective. The Headteacher, technician and admin team also monitor the school website, Class Dojo and Facebook page.

**Internet and Network Usage**

- Pupils use technology **only for educational purposes** under staff direction.
- Pupils access **class folders** and approved logins only (e.g. TT Rockstars, Teach Your Monster How to Read).
- **Mobile phones and smart watches** brought by pupils are stored in the school office unless for medical reasons.
- Staff use **school phones** for parent/pupil contact and avoid personal devices during the school day.
- Smart watches may be worn but **not used for communication**.
- Pupils use only **approved school accounts** for email, messaging and software.
- The school technician authorises staff devices for network access.
- Staff use **school email** for all professional communication.
- Pupils access the internet **only when instructed** by an adult.

**Protecting Personal Data**

- All personal data is stored securely in line with **GDPR**.
- Parents and pupils may request access to their data and corrections where appropriate.
- See the **GDPR Policy** for full details.

**Reporting a Concern**

- Concerns about pupil internet misuse are handled by the **Safeguarding Team or SLT**.
- Concerns about staff misuse go to the **Headteacher**.
- Safeguarding concerns follow the **Child Protection Policy** and are reported to a DSL.

# Published Content and Media

- Pupil images and information are used **with dignity and responsibility**.
- Only school contact details appear on the website.
- Parental permission is required for publishing photos or work; permissions are reviewed at entry, Year 3 and when policies change.
- Photos avoid full names and are selected carefully.
- Parents may take photos at events for **personal use only**, not for social media.

# Social Networking and Personal Publishing

- Access to social networking sites is **blocked/filtered** in school.
- Pupils learn about safe use, privacy settings and online footprints.

- Pupils are advised **not to use social networks unsupervised** and never to share personal details.
- Parents receive regular reminders through newsletters, the website and information evenings.
- Staff must **not add pupils or their families** on social media; any existing links must be declared to the Headteacher.

# Supporting Vulnerable Pupils

We provide additional support for pupils more at risk online (e.g. LAC, CP, CIN, SEND), including:

- Extra guidance available at Parents' Evenings.
- Additional support at the beginning of worship – key online safety messages shown on screen.
- Additional support posts on Class Dojo for specific areas of concerns (e.g. inappropriate apps or managing screen time)
- Links to trusted resources (e.g. NSPCC, Parent Zone, National College).
- Parent Online Safety sessions available through Coram/Scarf education.
- Support through PEP/Core Group/Multi-Agency meetings.
- Advice for parents on conversations to have at home.
- Help with understanding acceptable behaviour and seeking help.

# Monitoring and Review

- The policy is implemented daily by all staff and monitored by the **Headteacher**, **Online Safety DSL**, and **Computing Lead**.
- Governors review effectiveness regularly, ensuring Christian values remain central.
- Termly reviews involve the Computing Lead, DSL, Headteacher and relevant governors, with findings reported to the full governing body.