

Shurdington CofE Primary
Be the **BEST** we can be, through love.
Believe Enjoy Succeed Together
'Love God and love your neighbour as you love yourself.'
Matthew 22, verses 37 and 39.

Online Safety Policy

Shurdington Church of England policies are written in the spirit of Christian values

Agreed by Governors: Sept 26

Review Date: Sept 27

This Online Safety Policy addresses all rights, privileges and responsibilities associated with ICT, computing and the Internet. It encompasses Internet technologies and electronic communications such as mobile phones, as well as collaboration tools and personal publishing. It refers to the safe, acceptable and responsible use of the Internet, highlights the need to educate pupils about the benefits and risks of using technology, and provides safeguards and awareness for users to enable them to control their online experience.

The DSL will take responsibility for online safety and also ensure that there is an appropriate filtering system in place. As stated in 'Keeping Children Safe in Education' (KCSIE) 26, the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or other staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

The school's Online Safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Data Protection, AI and Security, Freedom of Information, Complaints, Child Protection, Race Equality, Disability Equality Plan, PSHCE and all other curriculum policies. It was written referencing relevant government guidelines including KCSiE 26 and the Governments "[Meeting digital and technology standards in schools and colleges](#)" guidance.

Purpose of this Policy

The Internet is an essential element in 21st century life for education, business, recreation and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management of information and business administration systems.

Contents

- Core Principles of the Online Safety Policy.
- The benefits of Internet access for education.
- Internet use at school.
- How pupils will learn to evaluate Internet content.
- How Internet access will be authorised.
- How the risks will be assessed.
- How complaints regarding Internet use will be handled.
- How filtering will be managed.
- Internet publishing statement.
- Management of website content.
- Newsgroups and chat.
- Social networking and personal publishing.
- Use of Artificial Intelligence (AI) systems in School
- Managing emerging Internet uses.
- Protecting Personal Data.
- Use of Portable Equipment.
- Personal Mobile devices.
- How ICT system security will be maintained.
- Introducing the policy to pupils.
- Staff consultation.
- Enlisting parents' support.
- Review.
- Regulation and guidelines.
- Parental Permission for Pupil use of Internet Facilities at School.

Core Principles of the Online Safety Policy

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Staff, pupils, parents and volunteers sign safe Use of Internet agreements.
- Sound implementation of the Online Safety policy in both administration and curriculum, including secure school network design and use.
- The Online Safety Policy and its implementation will be reviewed annually.
- Safe and secure broadband from the South West Grid for Learning and Gloucestershire Local Authority.
- All Internet access is filtered through a proxy server to screen out undesirable sites at source.
- National Education Network standards and specification.
- Informing parents/carers about the School's AUP.

The Benefits of Internet Access for Education

- The main reason we provide Internet access to our teachers and pupils is to promote educational excellence by facilitating resource sharing, innovation and communication. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Benefits of using the Internet in education include:

- Access to worldwide educational resources.
- Inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC) <http://vtc.ngfl.gov.uk>.
- Educational and cultural exchanges between pupils worldwide.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the LA and DCSF.
- Use of online workshops for enrichment of the curriculum.

All Internet users must do so within the boundaries of this policy and failure to do so may result in future internet access being denied.

Internet Use in School

The school will actively take all reasonable precautions to restrict pupil access to both undesirable and illegal material.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Rules will be displayed and there will be targeted lessons on Online Safety at the start of each new term.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils, including through the use of QR codes, in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How pupils will learn to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the DSL.
- The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught, through targeted lessons to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

How Internet access will be authorised

- At Foundation Stage Level, access to the Internet will be by adult demonstration. This will be with occasional directly supervised access to specific, approved online materials within the normal restrictions of a classroom.
- At Key Stage 1 and Key Stage 2 level, access to the Internet will be by adult demonstration. There will be supervised access to specific websites or to carry out specific web searches; using approved online materials within the normal restrictions of a classroom.

How the risks will be assessed

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Gloucestershire LA can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies recommended by SWGfL will be adopted.
- The Head Teacher will ensure that this policy is implemented and compliance with the policy monitored.

How complaints regarding Internet use will be handled

- Responsibility for handling incidents will be delegated to a member of the senior leadership team.
- Any complaint about staff misuse must be referred to the Headteacher in line with our complaints policy.
- Pupils and parents will be informed of the complaints procedure.

How filtering will be managed

- The school uses RM Safety Net (through the Southwest Grid for Learning) for its internet filtering.
- The school will work in partnership with parents; the Gloucestershire LA, the Department of Education and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the DSL.
- The DSL and Computing Co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Staff training includes understanding roles and responsibilities in relation to filtering and monitoring.
- The DSL/Headteacher will review filtering and monitoring reports where appropriate and ensure concerns are acted upon in accordance with safeguarding procedures.

Internet Publishing Statement

The school wishes the school's web site to reflect the diversity of activities, individuals and education that can be found at Shurdington C of E Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles will be adhered to:

- No video recording or photographs will be published without the written consent of the parents/legal guardian of the child concerned (signed on the child's behalf).
- Surnames of children will not be published in conjunction with photographic or video material.
- No link should be made between an individual and any home address.

- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. If in any doubt at all, refer to the Designated Child Protection Officer.

Management of Website Content

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and only used where parental permission has been given. Pupils' full names will not be associated with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This permission will be sought when the child first joins school and will cover all photographs whilst they are at Shurdington.
- The Head Teacher or Computing Co-ordinator will take overall editorial responsibility and ensure content is accurate and appropriate.

Social Networking and Personal Publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Use of Artificial Intelligence (AI) systems in School

- As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential. We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.
- We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.
- The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice. We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Staff should only use AI tools that have been approved by the school or appropriately risk assessed. AI systems should assist professional judgement and decision-making rather than replace it.

Managing Emerging Internet Uses

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones or smart watches are not allowed in school and, therefore, will not be used during lessons or formal school time.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available in accordance with UK GDPR and the Data Protection Act 2018.
- Personal data relating to pupils and staff will only be taken off site if necessary and then encrypted or password protected memory sticks will be used.

Use of Portable Equipment

The school provides portable computing equipment such as laptop computers, video recorders and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

- All equipment owned by the school is available for use by all staff. If it is in the care of an individual, access should be negotiated with the individual concerned. Any difficulties should be referred to the Computing Co-ordinator. All staff are expected to look after any equipment used and report any equipment that is not working properly to the Computing Co-ordinator. Faulty equipment, laptops or networking problems can also be logged in the 'Support Log'.
- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any computing equipment in their care to be returned to school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it.
- If an individual leaves the employment of the school, any computing equipment must be returned.
- The use of USB pens, re-writeable CDs, memory sticks etc. to transfer data from external computer systems must be virus free and encrypted.
- No other software may be installed on laptops in the care of teachers unless the school owns the licences.

Personal Mobile Devices

- The school allows staff to bring in personal mobile phones and devices for their own personal use.
- Mobile phones must not be used in view of the children unless a member of SLT has agreed permission. Mobile phones must not be used or shared in any way with the children. In emergencies, the school does allow a member of staff to contact a pupil or parent/carer using their personal device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device and that these devices are not used or shared with the children in any way.
- Pupils are not allowed to bring personal mobile devices/phones to school. In certain circumstances, pupils may be given permission to have a mobile device in school; the class teacher on receipt of a written request may give permission following a consultation with the Headteacher or a member of SLT. If permission is given then the device is to be kept in the school office.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

- Smart watches capable of photography, audio recording, messaging or internet access will be treated in the same way as mobile phones.

How ICT System Security will be maintained

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Use of data storage devices will be reviewed.
- If being used off site, all information or personal data about the children will be saved onto an encrypted memory stick, which will be provided by the school.
- Personal storage devices may not be brought into school without specific permission and a virus check.
- Files held on the school's network will be regularly checked.
- The Computing Co-ordinator will ensure that the system has the capacity to take increased Internet use.

Introducing the Policy to Pupils

- Rules for Internet access will be posted near all computer systems.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access and online safety will be taught, using our KAPOW Computing scheme regularly.
- A module on responsible Internet use will be included in the PSHCE programme covering both school and home use.

Staff Consultation

- All staff must accept the terms of the 'Acceptable Use Policy' before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Senior management should supervise the monitoring of Internet use is a sensitive matter.
- Staff development in the safe and responsible Internet use will be provided as required.
- Rules for responsible use of the Internet will be posted in the staffroom.

Enlisting Parents' Support

- Parents' attention will be drawn to this policy in newsletters, the school prospectus and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Remote Learning

- All stakeholders to be aware of the requirements of remote learning and how best to safeguard themselves.
- Pupils and staff will keep passwords safe and adhere to the requirements set out in their specific Acceptable Use Policy.
- All staff ensure they are aware of the requirements set out in the Remote Learning Online Safety Policy.

Monitoring and Review

The governing body will receive regular updates regarding online safety and the effectiveness of filtering and monitoring arrangements.

The governing body are aware of the need to keep this policy up to date and in line with current practice. Therefore, this policy will be monitored and reviewed annually.

Signed:

Signed:

Date:

Date:

Headteacher

Chair of Governors
