Online Safety Policy

"I am the vine, and you are the branches. If any remain in me and I remain in them, they produce much fruit."

John 15:5

Learning, growing and caring as part of God's family.

Jesus (the gardener) nourishes and tends us as we learn and grow, so that we can all flourish. As a vine, we are one, but all unique and special to Him. We care for each other, as God cares for us.

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education (2026), and relevant DfE guidance, including:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Keith Weatherill (Chair and Safeguarding Governor).

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Headteacher is responsible for reviewing the weekly filtering and monitoring reports generated by Netsweeper, provided through Lancashire Educational Digital Services, identifying any suspicious or potentially harmful online activity and ensuring that appropriate follow-up action is taken.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) [and deputies] are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Online Safety Lead to make sure the appropriate systems and processes are in place
- Working with the headteacher, Online Safety Lead and other staff, as necessary, to address any online safety issues or incidents
- Taking lead responsibility for safeguarding concerns arising from online safety incidents, ensuring that these are managed in accordance with the school's Child Protection and Safeguarding Policy.
- Ensuring that online safety incidents are recorded and managed appropriately, with safeguarding concerns relating to pupils recorded on CPOMS and other online safety

incidents recorded in the Online Safety Filtering and Monitoring Incident Log (Appendix 4), in accordance with this policy.
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

Online Safety Lead

The Online Safety Lead supports the Headteacher and Designated Safeguarding Lead (DSL) in promoting a positive culture of online safety throughout the school.
Responsibilities include:
- Supporting the implementation and review of the school's Online Safety Policy.
- Promoting online safety education across the curriculum.
- Supporting staff in delivering age-appropriate online safety teaching.
- Raising awareness of emerging online risks and developments in technology.
- Supporting communication with parents and carers about online safety.
- Working with the DSL and IT support provider to identify areas for improvement.

The DSL retains lead responsibility for safeguarding matters relating to online safety, including responding to concerns, managing incidents and overseeing the safeguarding aspects of filtering and monitoring.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL has lead safeguarding responsibility for filtering and monitoring arrangements, and being aware of how to report any incidents of those systems or processes failing by speaking to any DSL or deputy
- Following the school's agreed procedures for requesting access to blocked educational resources, with any changes authorised by school leaders and implemented by the appropriate ICT provider.
- Reporting online safety concerns promptly and ensuring that pupil safeguarding concerns are recorded on CPOMS, with other incidents recorded in Appendix 4 where appropriate
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix 1)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All primary schools are required to teach Relationships Education and Health Education. Online safety is also addressed through the Computing curriculum and other relevant areas of learning. In particular, pupils will be taught about:

- Misinformation, disinformation and AI-generated content.
- Online manipulation, harmful content and unhealthy online influences.
- Respectful online relationships, privacy and consent.
- Recognising and reporting online abuse, including inappropriate images.
- Developing critical thinking and digital resilience.

In Key Stage (KS) 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 (KS) 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

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

Staff must not intentionally view, copy, share or delete suspected indecent images of children. Any such concerns must be referred immediately to the DSL and managed in accordance with safeguarding guidance.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member, in conjunction with the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably

practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and seminudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Artificial intelligence (AI), including generative AI tools, is becoming increasingly accessible and has the potential to support teaching, learning and school operations. Scotforth St Paul's CE Primary and Nursery School recognises the benefits of AI whilst acknowledging the potential risks to safeguarding, privacy and online safety.

The school will promote the safe, responsible and appropriate use of AI technologies. In particular:

- **Safeguarding:** AI may be used to create or distribute harmful, misleading or inappropriate content, including realistic images, audio or videos (commonly known as 'deepfakes'). Any use of AI to bully, harass or harm others will be addressed in accordance with the school's Behaviour Policy and, where appropriate, Child Protection and Safeguarding Policy.
- **Data protection:** Staff must not enter identifiable pupil information, personal data or confidential school information into AI tools unless their use has been formally approved by the school and appropriate data protection safeguards are in place.
- **Responsible use:** Staff must exercise professional judgement when using AI-generated materials, checking their accuracy, suitability and appropriateness before using them in teaching or other school activities.
- **Use by pupils:** Any use of AI tools by pupils in school must be age-appropriate, supervised and supported by appropriate safeguards.
- **Risk assessment:** The school will consider safeguarding, data protection and other relevant risks before introducing new AI tools or systems, ensuring that appropriate measures are in place.

The school will continue to review its approach to AI as technology develops and further guidance becomes available.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendix 1 & 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendix 1 & 2.

8. Use of Photographs, Videos and Digital Images

Scotforth St Paul's CE Primary and Nursery School recognises the importance of photographs and videos in celebrating pupils' achievements, sharing learning experiences and communicating with parents and carers. The school is committed to ensuring that images of children are captured, stored and shared safely and appropriately.

All staff must follow the procedures outlined in this policy when taking, storing, using and sharing photographs and videos of pupils.

- Photographs and videos of pupils must only be taken and shared for legitimate school purposes, using school-approved devices and platforms. Personal devices must not be used unless specifically authorised by the Headteacher and appropriate safeguards are in place.
- Staff must check the relevant permissions and any safeguarding restrictions before sharing or publishing images.
- Images must not be shared through personal social media accounts, personal messaging services or other unauthorised platforms.
- Images must be stored securely in accordance with the school's data protection procedures and must not be retained on unauthorised personal devices.
- Particular care must be taken when identifying pupils in photographs, including the use of names or other personal information.
- Staff must follow the school's agreed procedures when sharing photographs and videos through ClassDojo, the school website, newsletters or other communication platforms.
- Any concerns about the inappropriate taking, storage or sharing of images must be reported promptly to the DSL or Headteacher.

The school will ensure that its practices reflect data protection requirements, safeguarding considerations and the permissions and restrictions recorded for individual pupils.

9. Use of Mobile Devices in School

Pupils are not permitted to use mobile phones or other personal smart devices, including smartwatches, during the school day, including breaktimes and lunchtimes. Smartwatches must not be worn during the school day. These arrangements support the school's commitment to maintaining a safe and focused learning environment.

Pupils may bring a mobile phone to school only with the prior agreement of the Headteacher or Deputy Headteacher, where this is necessary because they travel to and/or from school independently.

Where permission has been granted:

- Mobile phones must be switched off and handed to the class teacher on arrival at school.
- Phones will be stored securely by the class teacher throughout the school day and returned to pupils at the end of the day.
- Pupils must not access or use their phones while on school premises unless specifically authorised by the Headteacher or Deputy Headteacher.

Exceptions may be made in individual circumstances, including where a device is required for medical or accessibility reasons, following agreement with the Headteacher.

Any breach of these expectations, including the wearing or use of smartwatches during the school day, will be addressed in accordance with the school's Behaviour Policy. Where appropriate, devices may be confiscated and parents/carers contacted.

Any safeguarding concerns arising from the use of mobile phones or personal devices will be managed in accordance with the school's Child Protection and Safeguarding Policy.

Staff, volunteers and other adults working in school are expected to use personal mobile devices responsibly and in accordance with the school's Code of Conduct and Staff Acceptable Use Agreement. Personal devices must not be used in ways that compromise pupil safety, supervision or safeguarding.

10. Staff using work devices outside school

All staff members are responsible for taking appropriate steps to keep school-issued devices and the information stored on them secure when working outside school. This includes, but is not limited to:

- Keeping devices protected by strong, unique passwords or passphrases, in accordance with the school's ICT security requirements, and using multifactor authentication where required.
- Ensuring devices are locked when not in use and are not left unattended in insecure locations.
- Not allowing family members, friends or other unauthorised individuals to access or use school devices.
- Ensuring that school devices are used only for authorised work-related activities.
- Following the school's arrangements for securely accessing, storing and sharing school information, including personal and confidential data.
- Allowing security updates and other protective measures to be installed as required and not disabling or attempting to bypass security settings.

The school's external ICT provider is responsible for managing appropriate technical security measures on school devices, including encryption, antivirus protection and operating system updates.

Staff must not use school devices in any way that would breach the school's Acceptable Use Agreement (Appendix 2) or Data Protection Policy.

Any loss or theft of a school device, suspected unauthorised access, potential data breach or other security concern must be reported promptly to the Headteacher so that appropriate action can be taken, including contacting the external ICT provider where necessary.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Filtering and Monitoring

The school maintains appropriate filtering and monitoring arrangements to protect pupils from harmful and inappropriate online content and activity. The Headteacher and Designated Safeguarding Lead (DSL) work with the school's external ICT provider and Lancashire Educational Digital Services to ensure that these systems are effective and reflect the safeguarding needs of the school.

The Headteacher reviews weekly filtering and monitoring reports generated by Netsweeper, provided through Lancashire Educational Digital Services, including any suspicious or potentially harmful online activity. High-risk safeguarding concerns are escalated promptly in accordance with the school's safeguarding procedures, without waiting for the weekly review.

Online safety incidents and concerns are recorded and managed according to their nature. Safeguarding concerns relating to pupils are recorded on CPOMS and managed in accordance with the school's Child Protection and Safeguarding Policy. Other online safety incidents, including suspicious searches, inappropriate use of school devices or concerns identified through filtering and monitoring systems, are recorded using the Online Safety Filtering and Monitoring Incident Log (Appendix 4), where appropriate. Concerns involving staff conduct or safeguarding allegations about adults are managed through the relevant confidential procedures.

Filtering and monitoring arrangements are formally reviewed at least annually, and following significant changes to technology, identified safeguarding risks or concerns about system effectiveness. The review involves the Headteacher, DSL, external ICT provider, Lancashire Educational Digital Services where appropriate, and the responsible governor. Findings and any resulting actions are documented.

All staff are responsible for supervising pupils' use of technology, remaining vigilant to online risks and reporting concerns or failures in filtering and monitoring systems promptly.

This policy will be reviewed annually by the Headteacher and shared with the governing board. The review will be informed by an annual assessment of the online risks faced by pupils, recognising that technology and associated risks continue to evolve.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

Pupil Agreement/Online Safety Rules

***NB Parents/carers MUST read and discuss all the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.*

- I will only use ICT in school for school purposes
- I will only use the Internet and/or online tools when a trusted adult is present
- I will only use school-approved accounts and communication tools when using ICT in school.
- I will not deliberately look for, save or send anything that could be inappropriate or unpleasant
- I will not bring in inappropriate electronic materials from home
- I will not deliberately look for, or access inappropriate websites
- If I accidentally find anything inappropriate I will tell my teacher/trusted adult in school immediately
- I will only communicate online with people a trusted adult has approved
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not give out my own, or others' details such as names, phone numbers or home addresses
- I will not tell other people my ICT passwords
- I will not arrange to meet anyone that I have met online
- I will only open/delete my own files
- I will not attempt to download or install anything on to the school network without permission
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe. I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online safety
- I understand that failure to comply with this Acceptable Use Policy may result in being given consequences in line with the school's Behaviour Policy, including possible removal of access to use of ICT equipment.

We have discussed this Acceptable Use Policy with …….....
(print child's name) who agrees to follow the online safety rules and to support the safe use of ICT at Scotforth St Paul's Primary School.

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……

Pupil Class …….. Date……

Only when this AUP has been signed and returned will access to school ICT systems be allowed

Appendix 2: Policy for Acceptable Use of Digital Technologies- Staff and Volunteers

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy.

This acceptable use policy is intended to ensure:

- That staff and volunteers are responsible users of digital technologies for educational and professional purposes
- That school systems, digital resources and users are protected from misuse
- That staff and volunteers are protected from potential risk in using digital technology in school

All users of technology within our school must agree to certain rules and only use digital technology, resources and software as instructed.

Acceptable Use Policy Agreement

I understand that I must use digital systems and resources responsibly, to help ensure my own safety and the safety and security of other users and the school systems.

For my professional and personal safety:

- I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
- I understand that the school's digital technology resources and systems are primarily intended for educational use and that I will only use them for professional purposes or for uses specified within policies and rules set by the school.
- I will protect my login credentials by using strong, unique passwords or passphrases, keeping them confidential and using multifactor authentication where required. I will report any suspected compromise of my account promptly and follow the school's procedures for securing it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will be professional in my communications and actions when using digital systems and resources.
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will communicate with others in a professional manner.
- I will only take, store and share photographs or videos of pupils for legitimate school purposes, using school-approved devices and platforms, in accordance with Section 8 of the school's Online Safety Policy.
- I will check relevant permissions and safeguarding restrictions before sharing or publishing images of pupils, including through ClassDojo, the school website or other school communication platforms.
- I will not use personal devices to photograph or record pupils unless specifically authorised by the Headteacher and appropriate safeguards are in place.
- I will only use social networking sites in school in accordance with the school's policies.
- I will not engage in any on-line activity that may compromise my professional responsibilities or breach confidentiality
- I will use artificial intelligence (AI) tools responsibly and in accordance with the school's Online Safety Policy. I will not enter identifiable pupil information, personal data or confidential school information into AI tools unless their use has been formally approved by the school and appropriate data protection safeguards are in place. I will check the accuracy and suitability of AI-generated materials before using them for school purposes.

When accessing digital systems and resources:

- I will not connect personal devices to the school's network or ICT systems unless authorised to do so in accordance with the school's ICT security arrangements.
- I will only use devices and software authorised by the school and will not disable or interfere with security measures managed by the school's ICT provider.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- I will not try to use any tools or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
- I will not install or attempt to install software of any type on a machine nor attempt to change computer settings, unless this is permitted by the school
- I will handle personal and confidential information securely, in accordance with the school's Data Protection Policy. I will only access, use or share information where authorised and necessary for my professional responsibilities, and will report any suspected data breach promptly to the Headteacher.
- I will report any concerns about inappropriate online content, suspicious online activity or failures in the school's filtering and monitoring systems promptly to the DSL or Headteacher, in accordance with the school's reporting procedures.

When using the internet in my professional capacity:

- I will obtain the relevant permissions to use the work of others
- I will respect copyright and intellectual property rights when accessing, downloading, using or sharing digital materials, ensuring that any use is appropriately licensed or otherwise permitted by law.

I understand that I am responsible for my actions inside and outside of school:

- I understand that this acceptable use policy applies not only to my work and use of school technology equipment at school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

I understand that it is my responsibility to ensure I remain up to date and understand the school's most recent online safety and safeguarding policies.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed: …….

Role: …….. Date: ……

Appendix 3: Online Safety Training Needs – Self-audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you use strong, unique passwords and multifactor authentication (where required) when accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: Online Safety Filtering and Monitoring Incident Log

ONLINE SAFETY FILTERING AND MONITORING INCIDENT LOG				
Date	Where the incident took place	Description of incident	Action taken	Name and signature of staff member recording the incident

Approved by:	Curriculum Committee	**Date:** 21st Oct 2026
Last reviewed on:	October 2026	
Next review due by:	October 2027	
Changes		
19th October 2026	Pg 2 – KCSIE 2026 added Pg 3 – Headteacher role updated to reflect school filtering and monitoring arrangements; DSL role updated to reflect school recording arrangements. Pg 4 (and throughout document) – ICT Manager changed to Online Safety Lead and responsibilities updated; Staff and Volunteers section updates Pg 5 – Section updated to reflect statutory Relationships, Sex and Health Education 2026 Pg 8 – AI section updated Pg 9 – Section added: Use of Photographs, Videos and Digital Images; Use of Mobile Devices in School section updated Pg 10 – Staff use of work devices updated Pg 11 – Filtering and Monitoring section updated Pg 13 – Pupil Acceptable Use Policy updated Pg 14 – Staff Acceptable Use Policy updated	