St. Oswald’s Church of England Primary School

Online Safety Policy



***‘Teach children how they should live and they will remember it all their life.’***

**Proverbs 22:6**

Through basing our vision on the bible teaching above we will promote an inclusive school community, rooted in mutual respect, understanding and kindness towards others.

***‘Life in all its fullness.’***

**John 10:10**

In living out the statement above our vision is to develop resilience and a love of learning, which will enable the children to achieve their aspirations.

**Monitoring and Evaluation**

The Head Teacher shall have oversight of this policy and ensure all staff follow procedures and that these are carried out.

The effectiveness of this policy shall be monitored during Governor’s meetings. This policy will be updated annually and any changes occurring during the year should be updated as soon as possible.

|  |  |  |
| --- | --- | --- |
| Date approved | Next Review Date | Signed by |
| January 2022 | September 2023 |  |

**Policy Document for Online Safety**

1. Purpose
2. Audience
3. Communication of the Policy
4. Aims
5. British Values
6. Curriculum intent: What is online Safety?
7. What are the risks?
8. Definitions
9. Curriculum Implementation
10. Impact
11. Educating Parents
12. Information and Organisations
13. Roles and responsibilities
14. Parents and Carers
15. Visitors and Members of the Community
16. Handling Complaints
17. Cyber - bullying
18. Examining Electronic devices
19. Managing Internet Access
20. Physical Location Device Sitting
21. Email
22. Published content and the school web site
23. Publishing photographs, images and work
24. Social networking and personal publishing on the school learning platform
25. Staff using work devices outside school
26. Community use of the Internet
27. Managing emerging technologies
28. Other devices
29. Staff use of personal devices including mobile phones:
30. Other school stakeholders
31. Digital images and videos
32. Policy Decisions
33. Assessing Risk
34. How the school will respond to issues of misuse
35. Training
36. Links with Other Policies
37. Review and Monitoring Arrangements.
38. Appendix 1
39. Appendix 2
40. Appendix 3
41. Appendix 4
42. Appendix 5
43. **Purpose**

The purpose of this policy is to set guidelines for staff, pupils and parents on how devices, networks, websites and systems must be used. As a Christian school everything we do is driven by our Christion vision to promote an inclusive school community, rooted in mutual respect, understanding and kindness towards others.

1. **Audience**

This document is intended for all staff, school governors, LA inspectors/ consultants, parents and inspection teams. Copies are available on the staff shared drive and on the school website and available on request.

This policy will be part of the school induction pack for new staff

1. **Communication of this policy:**

**Staff and the Online safety policy**

* All staff will be given the School online safety Policy and its importance explained
* Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
* Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

**Introducing the online safety policy to pupils**

* Appropriate elements of the Online-safety policy will be shared with pupils
* Online safety rules will be posted in all networked rooms.
* Pupils will be informed that network and Internet use will be monitored
* Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils

**Enlisting parents’ support**

* Parents’ and carers attention will be drawn to the School online safety policy in newsletters, the school brochure and on the school web site.
* Parents and carers will from time to time be provided with additional information on online safety through our newsletter and through our website.
* The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
* Parents and carers will be reminded that they must not publish any images or comments of performances and other community events on social network sites before and after each event.
* Parents and carers will be reminded of online safety at school events.
1. **Our school aims to:**
* Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
* 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.
1. **British Values**

Through its ethos, curriculum, extra-curricular activities, teaching and learning St. Oswald’s Church of England Primary School will promote British values. By doing so, we will ensure that all learners understand the values that have traditionally underpinned British society. The implicit and explicit teaching of these values will promote cohesiveness within our school and community. St Oswald’s is proud to be part of the UN Convention of the Rights of the Child, where every child is valued, cared for and developed.

**This plan links to UNICEF Rights and Responsibility: Articles 16 & 17**

**Article 16: Right to privacy**

“Every child has the right to privacy.  The law should protect the child’s private, family and home life, including protecting children from unlawful attacks that harm their reputation …”

**Article 17: access to information from the media**

“Every child has the right to reliable information from a variety of sources, governments should encourage the media to provide information that children can understand.  Governments must help protect children from materials that could harm them.”

1. **Curriculum Intent**

**What is Online Safety?**

Online Safeguarding, internet safety, online safety and digital safeguarding are interchangeable but all relate to ensuring that those who use technology do so safely and responsibly. Typically, online safety tends to be associated with online grooming, online bullying or access to inappropriate images/video. However, there is a broader and developing agenda related to the growth of social media including information privacy, sexting, self-generated indecent content, gaming addiction, radicalisation and others. Online Safeguarding is a common thread running across related areas including child sexual exploitation, anti-bullying and anti-social behaviour.

Online Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It 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 school’s Online Safety policy should operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

At St Oswald’s we understand the online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats. It is therefore important to focus on the underpinning knowledge and behaviours that can help our pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching is built into existing lessons across the curriculum, covered within specific online safety lessons and also in other appropriate lessons. Our curriculum is designed to equip pupils with a sound understanding of risk and with the knowledge and skills necessary to make safe, fair and informed decisions.

All of the above is strongly underpinned by our vision as we encourage all of our children to show mutual respect and kindness to one another when using online devices. Similarly, we inspire all of our children to become resilient and responsible individuals when technology changes and knowing when rules need to be applied and followed. Having a deep understanding and knowledge of online safety is applicable to their everyday life both in school and at home and is something they will need to continue practising as they move through their education and into the world of employment.

1. **What are the risks?**

While recognising the enormous potential of technology and its applications, we need to accept that there are associated risks and develop effective mitigating strategies to address them. Different challenges will present on an on-going basis but the main risks can be considered to fall within specific categories.

**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, anti-Semitism, 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 semi-nudes and/or pornography), sharing other explicit images and online bullying; and

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

1. **Definitions**

**Copyright:** The exclusive legal right of the originator of print, publish, perform, film or record literary, artistic or musical material.

**Online bullying:** the use of ICT (information and communications technology – particularly mobile phones and the internet) to deliberately upset someone else.

**Digital Natives:** those born into and raised in the digital age.

**Digital Citizenship:** appropriate and responsible behaviour with regard to use of technology.

**Digital Footprint:** the term used to describe the trail, traces or "footprints" that people leave online. This is information transmitted online, such as forum registration, e-mails and attachments, uploading videos or digital images and any other form of transmission of information — all of which leaves traces of personal information available to others online

**Downloading:** receiving information electronically through the internet. This could include saving a document or picture from a website or media streaming e.g. music or video.

**Online safety:** The process of limiting risks to children and young people when they are using ICT. It is primarily a safeguarding issue and relates to all ICT fixed or mobile technologies, software, content and the internet or cloud services.

**Extremism**: defined in the 2011 Prevent strategy as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. Also included in the “Prevent” definition of extremism are calls for the death of members of our armed forces, whether in this country or overseas.

**Filtering:** software that can block access to specific websites and/or inappropriate material. No filtering can guarantee to be completely effective and other strategies including education and awareness raising need to be applied.

**Firewall:** a buffer between the computer and the internet which regulates both incoming and outgoing information.

**CPOMS: A system put in place to record incidents.**

**Online safety champions:** 3 children from year 6 and 2 children from each KS2 class.

1. **Curriculum Implementation**

**Educating Pupils about Online Safety**

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

The text below is taken from the National Curriculum computing programmes of study.

All schools have to teach:

* Relationships education and health education in primary schools
* Relationships and sex education and health education in secondary schools

In Key Stage 1, pupils will be taught to:

* Use technology safely and respectfully, keeping personal information private
* Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

* Use technology safely, respectfully and responsibly
* Recognise acceptable and unacceptable behaviour
* Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

* That people sometimes behave differently online, including by pretending to be someone they are not
* That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
* The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
* How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
* How information and data is shared and used online
* What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
* How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
1. **Impact**

The curriculum at St Oswald’s equips our pupils with the skills to live healthy, safe, productive, capable, responsible and balanced lives. Accurate information and sensitive teaching ensure our children are informed about online safety and issues of all kinds and that they are given honest information about their effects which will help them to make informed decisions in later life.

Through the curriculum our children are aware of the advantages of using online resources but understand that they need to be treated with care and used correctly, being mindful of their digital footprint. They also understand the legality and risks associated with the misuse of online resources and have accurate information regarding their effects. Online safety education contributes towards decreased harm and increased safety for young people, their families and communities. It enables pupils to build their confidence, resilience and self-esteem and to identify and manage risk. We believe, therefore, that our online safety education curriculum empowers our children to make informed choices resulting in long term benefits for them as citizens.

1. **Educating Parents**
* The school will raise parents’ awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
* Online safety will also be covered during parents’ evenings and other appropriate meeting sessions.
* If parents 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.
1. **Information and Organisations**

**CEOP:** The Child Exploitation and Online Protection Centre. Part of the Police they work to protect children from sexual abuse linking with international partners when required. CEOP develop and deliver resources to inform and educate about risk through the *Think U Know* educational programme.

**Childnet:** organisation that works in partnership with others to make the internet a safer place for children.

**Internet Watch Foundation (IWF):** Organisation that takes reports about illegal online content and are the “notice and take down” body for any content within their remit. Work in partnership with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimise the availability of content: child sexual abuse content anywhere in the world and criminally obscene and racial hatred content in the UK.

**UK Safer Internet Centre (UKSIC):** Partnership of three organisations: Childnet International, Internet Watch Foundation and South West Grid for Learning – three main functions: Awareness Centre, Helpline and a Hotline.

1. **Roles and Responsibilities:**

Online safety is not a discreet role and cannot be assigned to a single member of staff. Effective online safety is achieved through a whole school approach however there are some responsibilities which sit with a specific role in the school.

**The Headteacher:**

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

* Takes overall responsibility for online safety provision.
* Takes overall responsibility for data and security provision (Senior Information Risk Owner).
* Ensure the school uses an approved, filtered internet service which complies with current statutory requirements.
* Is responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues as relevant.
* Is aware of the procedures to be followed in the event of a serious online safety incident.
* Review regular monitoring reports from the Online Safety Co-ordinator.
* Ensures there is a system in place to monitor and support staff that carry out internal online safety procedures.
* The Headteacher is responsible for ensuring that the requirements of the Data Protection Act are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data and registrations are observed with the school.
* In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. This is particularly important with the increased use of computers and laptops at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act (GDPR).

**Governors and Online Safety Governor**

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

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

The governor who overseas online safety is Diane Haddock.

All governors will:

* Ensure that 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 (see appendix 1)

**School Business Manager/Administrator:**

* Ensures all personal and sensitive data held on office machines is appropriately protected through access controls (Information Asset Owner).
* Ensures that information held on office machines is done so in compliance with the Data Protection Act.

**Network Technician Agilysis**

* Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
* Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
* Conducting a full security check and monitoring the school’s ICT systems on a monthly basis
* Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
* Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

**School online safety Lead/Designated Child Protection Lead:**

Details of the school’s designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
* Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
* Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
* Updating and delivering staff training on online safety (appendix 5 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

**Computing Curriculum Lead:**

* Oversees the delivery of the online safety element of the computing curriculum.
* Liaises with the designated lead regularly to ensure online safety.
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
* Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

The ICT manager/Agylisis:

* Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
* Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
* Conducting a full security check and monitoring the school’s ICT systems on a weekly basis
* Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

**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 3), and ensuring that pupils follow the school’s terms on acceptable use (appendices 1 and 2)
* Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
* 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’

**Teachers:**

* Embed online safety awareness raising in all aspects of the curriculum and other school activities.
* Supervise pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities as relevant).
* Inform pupils about the use of the internet for research and ensure they are aware of legal issues relating to electronic content including but not exclusively copyright law.
* Understand and comply with the school policy on the use of phones, cameras and other mobile devices.
* Understand and comply with the school policy on the use of photographic images.
* Understand the importance of adopting good safety practise when using technology outside school and that the school online safety policy covers their actions out of school (if related to their membership of the school).
* New staff, during their induction, will be given information by our safeguarding lead and sign an acceptable use document.

**Pupils:**

* Take responsibility for learning about the benefits and risks of using the internet in school and outside.
* Read, promote and adhere to the Pupil Acceptable Use Agreement.
* Understand the need to avoid plagiarism and uphold copyright regulations.
* Understand the importance of reporting abuse, misuse or access to inappropriate materials.
* Understands what to do if they or someone they know feels worried or vulnerable when using online technology.
* Understand and comply with the school policy on the use of phones, cameras and other mobile devices.
* Understand and comply with the school policy on the use of photographic images and online-bullying.
* Understand the importance of adopting good online safety practise when using technology outside school and that the school online safety policy covers their actions out of school (if related to their membership of the school).
1. **Parents/Carers:**

Parents 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 (appendices 1 and 2)
* Parents can seek further guidance on keeping children safe online from the following organisations and websites:
* What are the issues? - [UK Safer Internet Centre](https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues)
* Hot topics - [Childnet International](http://www.childnet.com/parents-and-carers/hot-topics)
* Parent factsheet - [Childnet International](https://www.childnet.com/resources/parents-and-carers-resource-sheet)
1. **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).
1. **Handling complaints:**
* The school will take all reasonable precautions to ensure online safety but the rapid changes and expansion of technologies and content make it impossible to guarantee that inappropriate content will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed or any consequences thereof.
* Staff, pupils and other members of our school community have been made aware of this policy and are aware of potential implications of any infringement.
* Complaints concerning online bullying are dealt with in accordance with our Anti-bullying Policy. Complaints related to child protection are dealt with in accordance with our School and Local Authority child protection procedure.

**Handling Online safety complaint**

* Complaints of Internet misuse will be dealt with by a senior member of staff.
* Any complaint about staff misuse must be referred to the head teacher.
* As with other areas of school, if a member of staff, a child or a parent / carer has a complaint or concern relating to e-safety then they will be considered and prompt action will be taken. Complaints should be addressed to the online safety leader (Miss K Ledgerton) in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved.
* Incidents of online safety concern will be recorded using CPOMS and reported to the school’s designated safeguarding officer on duty at the time of the incident in accordance with school’s child protection policy. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy.
* Pupils and parents will be informed of the complaint’s procedure.
* Pupils and parents will be informed of consequences for pupils misusing the Internet. See appendix 2.

1. **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 one 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. Class teachers will discuss cyber-bullying with their classes and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. 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 so that 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

1. **Examining electronic devices**

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils’ electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a ‘good reason’ to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

* Cause harm, and/or
* Disrupt teaching, and/or
* Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

* Delete that material, or
* Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
* Report it to the police\*

\* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

* The DfE’s latest guidance on screening, searching and confiscation
* UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
* The school’s COVID-19 risk assessment

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

1. **Managing Internet Access**

**Information system security**

* School ICT systems security will be reviewed regularly and is managed by Agilysis.
* Agilysis maintains the security of the school network and is responsible for ensuring that virus protection is up to date at all times. However, it is also the responsibility of the IT users to uphold the security and integrity of the network by not using pen drives and not installing APPS and programmes without express permission from the online safety coordinator who will have checked with our Agilysis technician.
* Security strategies will be discussed with the Local Authority

**Internet access, security (virus protection) and filtering:**

**Managing filtering**

* The school will work in partnership with the local authority to ensure systems to protect pupils are reviewed and improved.
* If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher and the service provider (Agilysis) can block further access to the site immediately through remote access.
* The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Our School:**

* Has filtered secure broadband connectivity provided through the Council’s agreement.
* Uses internet filtering system (Smoothwall) which blocks sites by categories including (but not exclusively) pornography, race hatred, gaming, sites of an illegal nature. Our filtering solution provides user level filtering (pupils and teachers) where relevant, closing down or opening up options as appropriate to the age/key stage of the pupils.
* Has anti-virus software provided as part of the Council’s agreement and the network is set up so staff and pupils cannot download executable files.
* Uses Local Authority approved email systems which staff must use – personal email address are not to be used.
* Blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform.
* Only unblocks other external social networking sites for specific purposes and records when this has been the case and the reason.
* Has blocked pupil access to music downloads or shopping sites – except those approved for educational purposes at regional or national level.
* Works with the School Information and Technologies Strategic Board to ensure any concerns about the system are communicated to ensure the systems remain robust and protect users.
* Is vigilant and robust (in so far as it is practicable and reasonable) in its supervision of pupils.
* Ensures all staff and students have signed the acceptable use agreement and understands that they must report any concerns.
* Ensures pupils only publish within an appropriately secure environment
* Requires staff to preview websites before use (where they have not been previously viewed or cached) and signpost pupils to age and subject appropriate websites.
* Plans the curriculum context for internet use to match pupil age and ability using progressive online safety plans from SWGFL and also from our bespoke lessons written by MGL.
* Encourages the use of child friendly search engines where open internet searching is required, e.g. yahoo for kids, ask for kids or Google Safe Search.
* Does not allow or is vigilant when conducting “raw” image search with pupils e.g. Google Image Search.
* Informs all users that internet use is monitored.
* Informs staff and pupils that they must report and incident or failure of the filtering system immediately and staff must log the details (contact Agilysis) and track to resolution, escalating if necessary.
* Ensures that all users are aware of and understand the rules of appropriate use and the sanctions that may result from misuse.
* Provides advice and information to all members of the school community on how to report offensive materials, abuse and bullying.
* Reports any material suspected to be illegal to the appropriate authorities.

**Network Management (user access, backup)**

**Our school:**

* Uses individual, audited logins for all teachers and age appropriate log ins for students.
* Ensures the System Administrator/Network Manager (or the designated online safety lead as identified by the Head Teacher) is up to date with services and policies and requires the technical support provider to be up to date with services and policies.
* Storage of all data within the school conforms to the requirements of the Data Protection Act including the requirement for data stored online to conform to the EU Data Protection Directive where storage is hosted within the European Union.
* Ensures our technical provider is aware of and compliant with the Network Standards.
* The Data Protection Act requires that any personal data held on a part of the ICT system subject to disposal to be destroyed. Prior to the transfer or disposal of any ICT equipment the ICT technician must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.
1. **Physical Location Device Sitting**
	* Devices should be positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information.
	* Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
	* Equipment should be sited to avoid environmental damage from causes such as dust and heat;
	* Users should avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Part of the induction for new staff explains the importance of locking access if moving away from their device.
	* A ‘clear desk policy’ is in place, i.e. hard copies of sensitive data from our network are not left unattended on desks;
	* Users are be aware of the dangers of sending out sensitive data and should avoid the use of the internet and **pen drives are forbidden**.
2. **Email:**
* Our school provides staff with an approved email account for their professional use and makes it clear that personal email should be sent through a separate account. We do not publish email addresses of staff or pupils on the school website and use anonymised email accounts for communication with the wider public.
* We will consult with the Local Authority and if necessary contact the Police if any of our staff or pupils receives an email that we consider to be particularly disturbing or breaks the law. We will also report messages that appear to support illegal activities to the relevant authorities and if necessary to the Police.
* We ensure that ensure that email accounts are maintained and up to date and use technologies to protect users and systems against SPAM, phishing and viruses.

**Children**

* As part of online safety education pupils and staff may only use approved St Oswald’s e-mail accounts on the school system.
* Pupils must immediately tell a teacher if they receive offensive e-mail.
* As part of online safety education pupils will be advised not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
* Staff to pupil e-mail communication must only take place as part of lessons - via a school email address or from within the learning platform and will be monitored.
* As part of online safety education pupils will be advised that incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
* The school will consider how e-mail from pupils to external bodies is presented and controlled.
* The forwarding of chain letters is not permitted.

**Staff:**

* Staff are provided with an approved email system and know that this is the only email to be used for business purposes. Personal email addresses must not be shared with pupils or their parents/carers.
* Know they need to be particularly careful if they are required to send staff or pupil personal information. Secure systems such as S2S (for school to school transfer) or Collect should be used where possible. Further information is provided in the Information and Data Security Policy for Schools.
* Know that emails sent outside the school must be written carefully (and in some instances may require approval) in the same way as a letter written on school headed paper and emails should follow the school ‘house style’.
* Know that the sending of multiple or large attachments should be limited and may be restricted.
* Know the sending of chain letters and embedded adverts is **not** allowed.
1. **Published content and the school web site**
* The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
* The school website complies with the Statutory DFE Guidelines for Publications.
* Most of the material published on the website is the schools’ own work but where other work is published or linked to we credit the sources used.
* The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupil’s personal information will not be published.
1. **Publishing photographs, images and work**

Photographs that include pupils will be selected carefully as per consent given by parents and guardians. This will not enable individual pupils to be clearly identified.

* Pupils’ full names will be avoided on the Website or learning platform, as appropriate, including in blogs, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs or images of pupils are published on the school website or Twitter.
* Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
* Staff will not keep images of children on personal devices e.g. memory sticks or mobile phones, or use them for any use other than in school.
1. **Social networking and personal publishing on the school learning platform**
* The school will control access to social networking sites, and consider how to educate pupils in their safe use through online safety sessions. E.g. use of passwords.
* All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
* Pupils will be advised to use nicknames and avatars when using social networking sites.

Teachers must not run social network spaces for student use on a personal basis or to open up their own spaces to their pupils. The schools’ preferred system for communication with pupils must be used.

The school’s preferred system for social networking will be maintained in adherence with the communications policy.

**School staff will ensure that in private use**:

* No reference should be made in social media to students, pupils, parents/carers or school staff.
* They do not engage in online discussion on personal matters relating to members of the school community.
* Personal opinions should not be attributed to the school or local authority.
* Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.
* Parents, carers and pupils must not use social media to raise concerns or complaints – these should always be raised with the school directly.

1. **Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

1. **Community use of the Internet**
* All use of the school Internet connection by community and other organisations shall be in accordance with the school online safety policy.
1. **Managing emerging technologies**
* Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
1. **Other devices**
* Mobile phones and associated cameras will not be used during lessons or formal school time. Taking photographs at any time without the subject’s consent is prohibited. Any mobile phones brought into school by children will be turned off and handed in at the office until the end of the day.
* The sending of abusive, offensive or inappropriate material is forbidden.
* Staff should not share personal telephone numbers with pupils and parents.
1. **Staff use of personal devices including mobile phones:**
* Mobile phones and other mobile devices brought into school are done so entirely at the owners’ own risk. Our school accepts no responsibility for the loss, theft or damage of any phone or mobile device brought into the school.
* All mobile phone use is open to scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time if it is deemed to be necessary.
* Mobile phones and personally owned devices will be switched off or switched to “silent” mode. Bluetooth communication should be “hidden” or switched off.
* Mobile phones and personally owned devices will not be used during lessons or formal school time unless permission has been granted by a member of the senior leadership team for an emergency circumstance – they should be switched off or silent at all times. Staff may use their mobile devices during break times. If a staff member is expecting a personal call they can leave their phone with the school office to answer on their behalf or ask permission to use the phone other than at break times.
* Staff should not use personally owned devices, including mobile phones or cameras, to take photographs or videos of pupils and will only use work provided equipment for this purpose. In exceptional cases the Headteacher may give permission for personally owned devices to be used and in such cases the images must be transferred to the school network as soon as is practically possible and the media deleted from the device.
* No images or videos should be taken without the prior consent of the person or people concerned and that consent is informed and appropriate.
* Mobile phones and personally owned devices are not permitted in certain areas within the school site including changing rooms, toilets and in some settings bathrooms and changing areas.
* Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside the school in professional capacity. Staff will be given access to a school phone where contact with pupils or their family is required.
* Where a member of staff is required to use a mobile phone for school duties, for instance in the case of an emergency during off site activities or for contacting students or parents, a mobile phone will be provided and used. In an emergency where the member of staff doesn’t have access to a school owned device, they should use their own device and hide their own mobile number for confidentiality purposes. Guidance on how to do this is included in the useful links section.
* Staff mobile phones and other mobile devices may be searched at any time as part of routine monitoring.
1. **Other school stakeholders:**
* Mobile phones and other mobile devices brought into school are done so entirely at the owners’ own risk. Our school accepts no responsibility for the loss, theft or damage of any phone or mobile device brought into the school.
* All visitors are required to keep their phones on silent.
* Bluetooth or similar functions on a mobile phone should be switched off at all times and not used to send images or files to other mobile phones.
* Our school reserves the right to search the content of any mobile device on the school premises where there is a reasonable suspicion that it may contain undesirable material including (but not exclusively) pornography, violence or bullying.
1. **Digital images and videos**

In our school:

* We request parent/carer permission for the use of digital photographs or video involving their child/children as part of the school agreement form.
* We do not identify pupils in online photographic materials or include the full names of the pupils in the credits of any published school produced video materials, on DVDs or in image filenames.
* Our Staff Acceptable Use Policy includes a clause on the use of mobile phones or other personally owned mobile equipment for taking photographs of pupils.
* We obtain individual parent/carer or pupil permission (prior to publication) for long term use before individual pupil photographs (not group photographs) are used on the school website, in the school prospectus or in other high-profile publications.
* We block/filter access to social networking sites or newsgroups unless there is a specific educational purpose.
* We teach children to consider how to publish for wide range of audiences which might include their parents/carers, younger children, the school governor and the wider community as part of their Computing scheme of work.
* We teach pupils that they should be very careful about posting personal photographs on online network spaces and they are also taught how images posted online can be manipulated to cause upset. They are also taught to understand the need to maintain privacy settings to keep their personal information safe.
* We teach pupils that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with their images (including the name of the file) that reveals the identity of others and their location such as house number, street name or school. We teach them about the need to keep their information secure.
* We teach pupils about the need to respect themselves and other people in their online behaviour and tell them how to report bullying or abuse and what to do if they are worried.
1. **Policy Decisions**

**Authorising Internet access**

* All staff must read and sign the ‘Staff Code of Conduct for ICT’ before using any school ICT resource (Appendix 1).
* The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
* Parents will be asked to sign and return a consent form (Appendix 2).
* Pupils must agree to comply with the ‘Responsible Internet Use’ statement before being granted Internet access (Appendix 3).
* All adults not directly employed by the school will be asked to sign an ‘acceptable use of school ICT resources’ form before being allowed to access the Internet on the school site.
1. **Assessing risks**
* The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Sefton Children’s Services can accept liability for the material accessed, or any consequences of Internet access.
* The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.
1. **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 and ICT and internet acceptable use) 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

1. **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 the risks up
* Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSLs 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.

1. **Links with other policies**

This online safety policy is linked to our:

* Acceptable use policy
* Anti-=Bullying Policy
* Behaviour Policy
* Child protection and safeguarding policy
* Complaints procedure
* Computing Policy
* Data protection policy and privacy notices
* Staff Code of Conduct
* Remote learning policy
* Staff disciplinary procedures
1. **Monitoring arrangements.**

This policy will be reviewed every year by the online safety lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly

**Review and monitoring of this policy:**

This online safety policy has been reviewed by our school senior leadership team and is current and appropriate for its intended purpose and audience. It has been approved for adoption by the School Governing Body and has been communicated across the school community. The policy will be reviewed annually or earlier if there are significant changes to technologies or how they are used; any changes will be notified to the school community as they occur.

Appendix 1:

|  |
| --- |
| **Acceptable use of the school’s ICT systems and the internet: agreement for staff, governors, volunteers and visitors** |
| **Name of staff member/governor/volunteer/visitor:**  |
| When using the school’s ICT systems and accessing the internet in school, or outside school on a work device, I will not: * Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
* Use them in any way which could harm the school’s reputation
* Access social networking sites or chat rooms
* Use any improper language when communicating online, including in emails or other messaging services
* Install any unauthorised software
* Share my password with others or log in to the school’s network using someone else’s details
 |
| I will only use the school’s ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.I agree that the school will monitor the websites I visit.I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy.I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.I will always use the school’s ICT systems and internet responsibly, and ensure that pupils in my care do so too. |
| **Signed (staff member/governor/volunteer/visitor):**  | **Date:** |

###### Appendix 2:

|  |
| --- |
| **Acceptable use of the school’s ICT systems and internet: agreement for pupils and parents/carers** |
| **Name of pupil:**  |
| **When using the school’s ICT systems and accessing the internet in school, I will not:** * Use them for a non-educational purpose
* Use them without a teacher being present, or without a teacher’s permission
* Access any inappropriate websites
* Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
* Use chat rooms
* Open any attachments in emails, or follow any links in emails, without first checking with a teacher
* Use any inappropriate language when communicating online, including in emails
* Share my password with others or log in to the school’s network using someone else’s details
* Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
* Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:* I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher’s permission
* I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit.I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.I will always use the school’s ICT systems and internet responsibly. |
| **Signed (pupil):**  | **Date:** |
| **Parent/carer agreement:** I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. |
| **Signed (parent/carer):**  | **Date:** |

**Appendix 3:**

**St. Oswalds CE Primary School’s Online Safety Rules**

These Online safety Rules help to protect students and the school by describing acceptable computer use.

* I understand the school owns the computer network and learning platform and can set rules for its use to keep me safe.
* I will only use ICT systems in school, including the internet, email and digital pictures for school purposes.
* I will only log on with my own user name and password.
* I will not share my passwords with anyone.
* I will only use my school email address at school.
* I will make sure that all messages are responsible, respectful and sensible.
* I will be responsible for my behaviour when using the Internet/learning platform. This includes resources and the language I use.
* I will use the forums on the school’s learning platform for sharing information sensibly.
* I will not give out any personal information about myself or anyone else when using the internet.
* If I accidentally come across any material that makes me uncomfortable I will report it to a teacher.
* I will not download or install software.
* I will respect the privacy and ownership of others’ work on-line at all times.
* I understand the school may watch my use of the school’s computer systems and learning platform.
* I understand that I will only be allowed to use the school equipment and systems by following these rules.

**Pupil name:** ………………………………….......……………………………………….

**Pupil signature:**…………………………………………… **Date:**……………

# Appendix 4:

|  |
| --- |
| **Online safety incident report log** |
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix 5:

|  |
| --- |
| **Online safety training needs audit** |
| **Name of staff member/volunteer:** | **Date:** |
| 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?  |  |
| Do you regularly change your password for 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? Please record them here.  |   |