Online Safety Policy 2026-27

Our Light Shines Always

We want the best teaching, the best opportunities and the best support and encouragement for every child. We are a friendly, happy, Catholic school, where everyone is valued for their individuality and special gifts.

Named personnel with designated responsibility for Online Safety

Academic year	Designated Lead	Chair of Governors	Review Dates
2025-26	Chris Wallace	Hugh Stolliday	September 2026
2026-27	Chris Wallace	Hugh Stolliday	September 2027

Introduction

Issue date:	September 2026
Reviewed by:	Chris Wallace
Review date:	September 2027

Senior Manager with responsibility for whole school ICT:	Sam Henzell
ICT Subject Leader:	Chris Wallace
Safeguarding Responsibility:	SLT / DSL's
Technician:	Bishop Bewick Trust

Monitoring of the Information and Communication Technology (ICT) policy is the responsibility of the ICT Team and Senior Management of the school.

The policy is reviewed each year by the ICT Team and Senior Leadership Team and fully revised and presented to Governors for final approval every three years before being issued to staff.

As Online Safety is an important aspect of strategic leadership within the school, the Head Teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety Coordinator in this school is Chris Wallace who has been designated this role. All members of the school community have been made aware of who holds this post. It is the role of the Online Safety Coordinator to keep abreast of current issues and guidance through organisations such as Newcastle Local Authority, Department for Education, Child Exploitation and Online Protection Centre (CEOP), and Childnet. Senior Management and Governors are updated by the Head Teacher and Online Safety Coordinator and all governors understand the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies:

- Child Protection
- Health and Safety
- Home - School Agreements
- Behaviour / Pupil Discipline (including the Anti-Bullying)
- PSHCE
- Corporate ICT Policies

2.0 Teaching and learning

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- Access to world-wide educational resources, including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across networks of schools, support services and professional associations
- Improved access to technical support including remote management of networks and access to learning wherever and whenever convenient

Our aim is to produce learners who are confident and effective users of ICT. We strive to achieve this by:

- Helping all children to use ICT with purpose and enjoyment
- Helping all children to develop the necessary skills to exploit ICT
- Helping all children to become autonomous users of ICT
- Helping all children to evaluate the benefits of ICT and its impact on society
- Meeting the requirements of the National Curriculum and helping all children to achieve the highest possible standards of achievement
- Using ICT to develop partnerships beyond the school
- Celebrating success in the use of ICT

2.1 Why is Internet use important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed, ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhance the school's management information and business administration systems.

2.2 How does Internet use benefit education?

Increased computer numbers and improved Internet access may be provided but its impact on pupils' learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and refine their publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- The school's Internet access will be designed to enhance and extend education
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work

2.3 How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content; for example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of online materials is part of teaching/learning in every subject

3.1 How will email be managed?

- Pupils are not expected to have e-mail accounts from school. Their Teams logins may look like an e-mail address, but they are set up as to not send or receive e-mail.
- Pupils will be taught that they must not reveal personal details of themselves or others in email communication, or arrange to meet anyone.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school
- Access in school to external, personal email accounts may be blocked
- Staff should use work email address for professional emails.

3.2 School website

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information **must not be published**
- The Headteacher will take overall responsibility and ensure that content is accurate and appropriate
- All comments on the blogs should be approved by teachers before being published.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright

3.3 Can pupil's images or work be published?

- We will only use images of children for whom consent has been given.
- Pupils' full names will not be used anywhere on the website. We will use Christian names only.
- Written permission from parents or carers must be obtained before images of pupils are electronically published
- Children's work may be published on the school website.

3.4 How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice if classroom use is to be developed, as well as assessing its worthiness to the education of the children.

3.5 Mobile Phones

Mobile phones are now a feature of modern society and many of our pupils own one. The school recognises the advantages mobile phones have as a ubiquitous learning tool. However, this new technology is open to abuse leading to the invasion of privacy.

Increasing sophistication of mobile phone technology presents a number of issues for schools:

- They are valuable items that may be stolen
- The integration of cameras into phones leading to potential child protection and data protection issues
- The potential to use the phone e.g. for texting whilst on silent mode
- Inappropriate messages being sent via SMS, including Cyberbullying and sexual harassment
- Interruption to lessons and disrupting the learning of others
- If phones are brought into school, phones must always be switched off (not on silent mode) and handed in to the main office before the start of the school day, to be collected at the end of the day.
- If a pupil needs to contact his/her parents/guardians they will use a school phone in the main office.
- If parents need to contact children urgently they should always phone the school office
- School accepts no responsibility whatsoever for theft, loss, damage or health effects, (potential or actual), relating to mobile phones.
- If a pupil breaches these rules the phone will be confiscated and given in to the main office. It will be returned to the pupil's parents. If another offence is committed then the phone will be confiscated and will only be returned to that pupil's parent/guardian in person with clear instructions on what is the correct procedure for mobile phones.
- Visiting adults to the school will be told to leave phones either in the office or in a locker in the staffroom. They will not be permitted to use them beyond the staff area.

3.6 Laptops/iPads

- Staff provided with a laptop/iPad purchased by the school can only use it for private purposes at the discretion of the Headteacher. Such hardware remain the property of the school and are open to scrutiny by senior management, contracted technicians and the ICT subject leader.
- Laptops/iPads belonging to the school must have updated antivirus software installed and be password protected.
- Staff intending to bring personal laptops on to the school premises should consider whether this is appropriate. There are security risks associated with any private content on the laptop

- Staff should not attach personal laptops to the school network, without permission from the SLT/ICT Technician.
- The security of school laptops/iPads is of prime importance due to their portable nature and them being susceptible to theft

4.1 Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's computers and ICT equipment
- All staff must read and sign the 'Acceptable use for staff agreement' before using any school ICT resource
- Parents will be asked to sign and return a consent form for pupil access
- Parents will be informed that pupils will be provided with supervised Internet access (see Appendix II)

4.2 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material through the use of corporate filtering systems. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never appear on a computer connected to the school network. The school or Newcastle Local Authority does not accept liability for any material accessed, or any consequences resulting from Internet use
- The final decision when assessing risks will rest with the Headteacher
- Teachers will freeze the boards when making any searches on the internet.
- Staff must exercise caution when visiting non-filtered sites such as Youtube and any videos (from this or other video streaming sites) must be checked before use in the classroom.
- No content that is rated above the age of the pupils watching may be accessed or shown to children. No content rated 12+ may be shown in school. Content rated at PG must be checked before viewing. For films, searching the BBFC website gives a breakdown of any content within the film.

4.3 Handling Online Safety complaints

- Complaints of ICT/Internet misuse must be recorded and will be dealt with by a senior member of staff, who will decide if sanctions are to be imposed
- Any complaint about staff misuse must be referred to the Headteacher who will decide if sanctions are to be imposed
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- The Headteacher will arrange contact/ discussions with Newcastle Local Authority and the police to establish clear procedures for handling potentially illegal issues
- Any complaint about illegal misuse must be referred to the Headteacher, who will decide if a referral to the police or other relevant authority is necessary, following any guidelines issued by Newcastle Local Authority
- All staff, pupils and parents will be informed of the complaints procedure

- All staff, pupils and parents will be informed of the consequences of misusing the Internet and ICT equipment

4.4 Cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's Anti-Bullying Policy
- There will be clear procedures in place to support anyone affected by Cyberbullying
- All incidents of Cyberbullying reported to the school will be recorded in CPOMS.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary

Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive
- A service provider may be contacted to remove content
- Internet access may be suspended at school for the user for a period of time
- Parent/Carers may be informed
- The police will be contacted if a criminal offence is suspected

4.5 Managing the School Website (including social media)

- Senior Leadership Team and staff will monitor the usage of the news pages by parents / pupils (comments) and staff regularly in all areas, in particular communication tools and publishing facilities
- Pupils/staff will be advised on acceptable conduct and use when using the website and social media.
- Only members of the current pupil and staff community will have access to the school social media groups.
- All users will be mindful of copyright issues and will only upload appropriate content onto the website and blogs.

Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive
- The material will be removed by the site administrator if the user does not comply
- Access to the school social media groups and website for the user may be suspended at the discretion of the SLT

- The user will need to discuss the issues with a member of SLT before reinstatement
- A pupil's parent/carer may be informed

4.6 Technical

Despite careful design, filtering systems cannot be completely effective so levels of supervision and access will depend on the child's age and experience. Due to the scale of content, neither the school, trust or Newcastle City Council can accept liability for the material accessed or any consequence of internet access.

- Internet access is filtered for all users. Content is filtered by the broadband provider along with Newcastle City Council filtering software.
- Each child will be given a specific numbered laptop / ipad so that users can be monitored.
- Pupils will be made aware of the importance of filtering systems through digital literacy lessons and will be warned of the consequences of attempting to subvert the filtering system.
- If staff or pupils discover an unsuitable website, the URL (web address) and content must be reported to either the Online Safety Co-ordinator or Newcastle City Council.
- Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e headteacher, LADO, police, Internet Watch Foundation.
- The use of Newcastle Council filtering systems may change during the year if an improved offering is available.

4.7 Social Media

School staff should be aware of what they have placed online on their own social media profiles and should take reasonable steps to minimise any risk of harm to pupils, staff and the school by:

- Ensuring that personal information is not published.
- No reference is made to students/pupils, parents/carers or school staff.
- Not engaging in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school, trust or local authority.
- Checking security settings to make sure their information is safe and only accessed by those who have been allowed (e.g. friends)

When official school social media accounts are used there should be:

- Approval from senior leaders

- Clear process for the administration and monitoring of these accounts, involving at least 2 members of staff.
- A code of behaviour for users of the account including systems of reporting and dealing with abuse and misuse and understanding of how incidents may be dealt with under school disciplinary procedures.
- As part of active social media engagement, it is good practice to pro-actively monitor the Internet for public postings about the school and effectively respond according to a defined process.

5.1 Sharing with pupils

- Online Safety rules and posters will be displayed in all rooms where computers are used and highlighted/ discussed during ICT sessions
- Pupils will be made aware that the network and Internet use will be monitored
- Teaching staff will be trained annually on Online Safety.
- As part of the Computing curriculum, implemented in 2014, all children will be taught a module of Digital Literacy using a bespoke scheme of work and Pol-Ed, created by the Police.

The programme of study for KS1 is: **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.**

The programme of study for KS2 is: **Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact**

5.2 Sharing with staff

- Staff will be consulted when creating and reviewing the Online Safety policy
- Staff training in safe and responsible Internet use, both professionally and personally, will be provided, including use of social networking sites such as Facebook
- Every member of staff, whether permanent, temporary or supply, will be informed that Network and Internet traffic will be monitored and can be traced, ensuring individual accountability

5.3 Engaging parents

- Parents'/ carers' attention will be drawn to the School Online Safety Policy at the beginning of the year when agreeing to Internet use for their child by signing an acceptable use policy and on the school website
- A parents' workshop will be held annually to inform parents/ carers about Online Safety issues and responsible use
- Parents will be requested to sign an Online Safety/Internet agreement as part of the Home School Agreement (Appendix III)
- Information and guidance on Online Safety will be made available to parents/carers in a variety of formats (i.e. weblinks, printed documents,

leaflets, presentations)

- In accordance with guidance from the Information Commissioners office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on social media sites.

6.1 Dealing with Unsuitable / Inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school/academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school/academy context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school/academy context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X

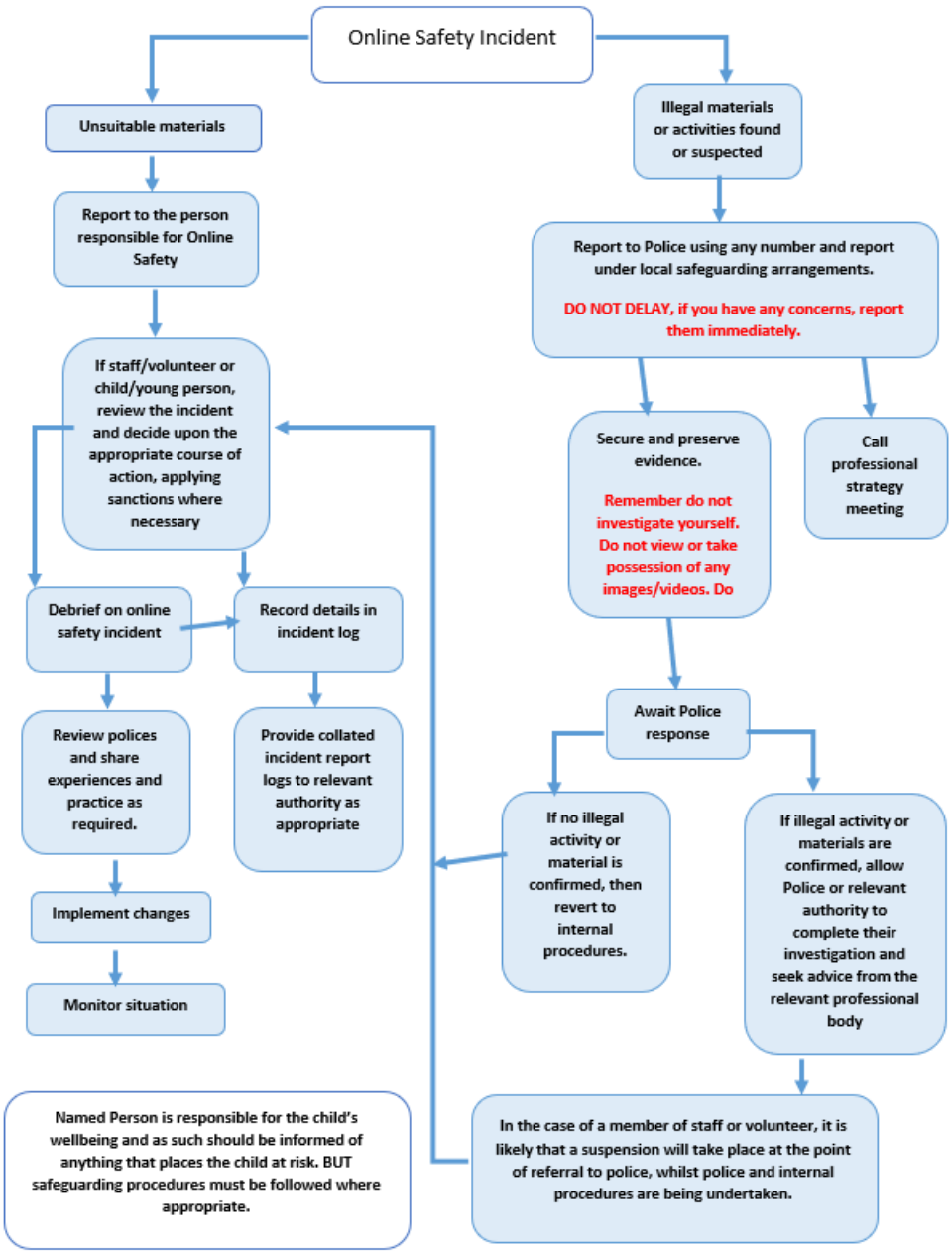
upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce				X	

File sharing				X	
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube			X		

6.2 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



6.3 Other Incidents

It is hoped that all members of the school/academy community will be responsible users of digital technologies, who understand and follow school/academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Acceptable Use Agreement for Staff

Computing and the related technologies such as e-mail, the Internet and mobile devices form part of our daily life within school. To ensure that all adults within the school setting are aware of their responsibilities when using any form of ICT all staff must sign this Acceptable Use Agreement and adhere to its content at all times. This is to ensure staff provide positive role models to pupils for the safe and responsible use of online technologies and also safeguard themselves from any potential allegations or inadvertent misuse.

- I know that I should only use the school equipment in an appropriate manner and for professional use in accordance with the Online Safety Policy
- I will keep my mobile phone in the staff areas (office, meeting room and staffroom) unless I have permission from the Headteacher.
- I will not give out personal information (mobile phone number, personal e-mail address etc) to pupils or parents
- I will only use the approved, secure e-mail system (name@olsa.org.uk) for any school business
- I know that I should complete virus checks on my laptop, memory stick and other portable devices so that I do not inadvertently transfer viruses onto the school network or other ICT equipment
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will ensure school data is stored securely and used appropriately in accordance with school and other relevant policies
- I will report any accidental misuse of school ICT, or accidental access to inappropriate material, to the Computing Subject Leader or Headteacher
- I will not connect any personal device (laptop, digital camera etc), to the school network without authorisation from the Headteacher
- I will respect copyright and intellectual property laws
- I understand that all my use of the Internet and other related technologies can be monitored and logged and made available to the Headteacher
- I will ensure that my online activity, both in and outside school, will not bring myself or the school into disrepute (this includes postings on social networking sites e.g. Facebook)

I have read, understood and agree to this code of conduct. I will support the safe and secure use of ICT throughout the school. I am aware I may face disciplinary action if I fail to adhere to it.

Signature: _____ Date: _____

Print Name:_____

Code of Conduct for Pupils

I agree to follow these rules when using the Internet:

- I will not share my username, password or personal information with anyone else
- I will make sure that ICT communication with other users is responsible, polite and sensible
- I will not look for, save or send anything that could be upsetting or cause offence. If I accidentally find anything like this I will tell a teacher immediately
- I will only upload materials which are free from copyright and suitable for school use
- I will not deliberately misuse or deface other users' work on the school network
- I know that my use of the Internet is monitored and further action may be taken if a member of school staff is concerned about my safety
- I will be responsible for my behaviour when using the Internet because I know that these rules are designed to keep me safe
- If I bring my phone into school, I will hand it in to the main office before the start of the school day and collect it at the end of the day. (Only where absolutely necessary and agreed with the headteacher)
- I understand and agree to the rules above and am aware there may be sanctions if I do not follow them

Signed: _____

Class: _____

Date: _____

Supporting Letter

Dear Parent / Carer

In order to support the school in educating your child about Online Safety (safe use of the Internet), please read and discuss the Online Safety rules attached with your child then sign and return the slip below.

Should you have any concerns and wish to discuss the matter further please contact Mr Wallace via the school office.

Yours Sincerely

Mrs Henzell

Headteacher

✂_____

Online Safety Acceptable Use Rules Reply Slip

I have read and discussed the rules with _____ (child's name) and confirm that he/ she has understood what the rules mean and agrees to follow the Online Safety rules to support the safe use of ICT at Our Lady and St Anne's Catholic Primary School.

Parent/ Carer
Signature: _____

Print name: _____

Date: _____

Laptop/Ipad Policy for Staff

Staff provided with a laptop purchased by the school, agree to the following terms of use:

1 The laptop/iPad remains the property of Our Lady and St Anne's Catholic Primary School and is for the use of the person it is issued to and must be returned to the school if and when the teacher leaves employment at the school.

2 The laptop/iPad is open to scrutiny by senior management, contracted technicians and the ICT Subject Leader at school.

3 Acceptable Use – teachers should accept and adhere to the school's Acceptable Use Policy, particularly with regard to Internet access.

4 The loading of additional software and APPs must be authorised by the school , support teaching and learning and be compliant with the following regulations:

- **Copyright, Designs and Patents Act 1988**
  Specifies that all software must be used only in accordance with the terms of the licence. Generally, the making of copies is forbidden and is a criminal offence.

- **Computer Misuse Act 1990**
  Identifies three main offences concerning unauthorised access to systems, software or data.

If you are in any doubt please speak to your school or LA before loading any software

5 Anti-Virus software must be installed and should be updated on a regular basis. The ICT technician will advise on the routines and schedule of this operation.

6 Staff are responsible for updating and maintaining the iPad/Laptop. Any queries should be addressed to the ICT technician or Computing Coordinator.

7 All repair and maintenance of laptops must be conducted under the terms and conditions of the warranty.

8 Data Protection – the terms of the school's Data Protection registration should be adhered to and users must clearly understand that there is a personal legal duty on them as well as the school.

9 Any charges incurred by users accessing the Internet from home are **not** chargeable to the school.

10 Staff should not connect personal laptops onto the school network without the permission of the Headteacher.

11 Failure to comply with these guidelines and the school's Acceptable Use Policy, may result in the withdrawal of the laptop and may lead to disciplinary proceedings.

***Laptop/iPad Details**:*

Make: _____

Model: _____

Serial Number: _____

***Authorised by Headteacher**:*

Signed: _____

Date: _____

***Member of Staff**:*

Print name: _____

Signed: _____

Date: _____

Mobile Phone Policy

- Our Lady and St Anne's Catholic Primary School discourages pupils from bringing mobile phones to school
- If a pupil needs to bring a mobile telephone to school, a request needs to be made to the Headteacher. The phone will be kept in the office or Headteacher's office.
- If a pupil needs to bring a mobile telephone to school for one day in an emergency, parents need to seek verbal permission from the Head or Deputy Headteacher
- The phone must be clearly labelled with the child's name, switched off and given in to the office on arrival at school
- The phone must be collected at the end of the school day from the office
- Where a pupil is found with a mobile in school, including the playground, the phone will be taken from the pupil and placed in the office. Parents will be contacted to collect the phone.
- If a pupil is found taking photographs or video footage with a mobile phone of either pupils or teachers, this will be regarded as a serious offence and the Headteacher will decide on appropriate disciplinary action. In certain circumstances, the pupil may be referred to the Police. If images of other pupils or teachers have been taken, the phone will not be returned to the pupil until the images have been removed by an appropriate person.
- Parents are advised that Our Lady and St Anne's Catholic Primary School accepts no liability for the loss or damage to mobile phones which are brought into the school
- If a pupil needs to contact his/her parents/guardians they will be allowed to use a school phone. If parents need to contact children urgently they should phone the school office and a message will be relayed promptly.
- Staff are discouraged from taking mobile phones into the classroom. If a phone needs to on in the classroom, (for personal reasons) staff need to seek verbal permission from the Headteacher, Business Manager or an Assistant Headteacher.

This policy became operational from September 2022

The policy may be amended from time to time in accordance with school development and any changes to legislation.

Our Lady and St Anne's Catholic Primary School

Parental Consent Form

At Our Lady and St Anne's RC Primary School we strive to provide innovative, high quality learning opportunities as part of broad and enriched curriculum. To this end we require your permission for your child to participate in a number of activities while they are here.

Please complete and sign.

1. INTERNET ACCESS – Acceptable Use Agreement

As part of the school's ICT programme we offer pupils supervised access to the internet. In order to reduce the risk of accidentally accessing inappropriate material, the school employs a service provider that prevents access to listed undesirable sites; however, no system is fool-proof. We require your written permission fo your child to have access to the internet.

I understand that my child will use the internet at school. I understand that the school will take all reasonable precautions to ensure that my child does not gain access to inappropriate material. I understand that pupils will be held accountable for their own actions.

2. USING IMAGES OF CHILDREN

There will be occasions when your child is photographed or filmed taking part in school activities. We seek your permission to use your child's image for display within the school, on our website or to accompany newspaper articles.

I give permission for my child's image and their work to be used on the school website.

I give permission for my child's image to be used for promotional purposes such as in the school prospectus or to accompany newspaper articles

I give permission for my child's first name to appear alongside their work/photo.

3. **THE USE OF FILMS AND VIDEO CLIPS RATED PG**

We like to make use of modern technologies throughout the curriculum and sometimes take the opportunity to use feature films and associated resources for education or enrichment activities. There are occasions when the materials have been classified PG. We ask your permission to use PG rated films that we deem to be acceptable for the age, maturity and well-being of your child.

I give my permission for my child to watch films and clips that have a PG classification.

Child's Name: _____

Signed_____Date_____

(parent/guardian)

This will be kept on file for the whole time that your child is at school

Appendix VII

Legal Requirements

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation, in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as “Sexting”). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.

More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files)
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks)

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is

usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material, with a view of releasing it, a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess “extreme pornographic image”

63 (6) must be “grossly offensive, disgusting or otherwise obscene”

63 (7) this includes images of “threats to a person’s life or injury to: anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”

Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Head Teachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy

Appendix VIII

Further Information and Guidance

School Website

http://olsa.org.uk/website

BBC

https://www.bbc.com/ownit

CEOP (Child Exploitation and Online Protection Centre

www.ceop.police.uk

Childline

www.childline.org.uk

Childnet

www.childnet.com

Cybermentors

www.cybermentors.org.uk

Digizen

www.digizen.org.uk

Information Commissioner's Office

www.ico.gov.uk

Internet Watch Foundation

www.iwf.org.uk

School Improvement service

Ian Clennell (Safeguarding Adviser)

ian.clennell@newcastle.gov.uk

Think U Know website

www.thinkuknow.co.uk