

Online Safety Policy

Document Title	Online Safety Policy
Lead Officer:	Head teacher
Approving Body:	Longford Board of Governors
Review Date:	Annually (and whenever change is required)
Edition and Date approved:	Edition 3 : April 2022
Indicate whether the document is for public access or internal access only <i>(Strikethrough text, as appropriate)</i>	Public Access – PDF copy to be posted on School website Internal Access Only – copy to be held on School PC <i>A back-up copy of all Policies is retained by the Clerk to the Longford Board of Governors</i>
Indicate which legislation or statutory guidance document requires this Policy	
Summary/Description:	
This document enables Longford Primary School to provide pupils with as safe an Internet environment as possible and guidelines to teach them to be aware of and respond responsibly to the risks.	

Longford CofE Primary School Online Safety Policy

1. Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using computing. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones. Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill.

The e-Safety Policy relates to other policies including those for Computing, Anti-Bullying and Child Protection. In line with these policies, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

The school's e-Safety Coordinator is the Headteacher, although every member of staff has a responsibility for ensuring children are kept safe and would need to act if an e-safety issue arose. The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires from pupils, parents and staff

Why is Internet use important?

The purpose of Internet use in school is to:

- raise educational standards
- promote pupil achievement
- promote well-being
- support the professional work of staff
- enhance the school's management information and administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

2. Leadership and Management

2.1 Authorised Access

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission will be sought at least at the start of each academic year or when a child starts at the school.

The school receives Internet Service Provision (ISP) from South West Grid for Learning (SWGfL) and has a service which proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances.

The school receives Internet Service Provision (ISP) from 'Schools Broadband' and will request monitoring reports from the ISP which will be regularly checked to identify any attempts to access illegal content and should notify the local police and Wiltshire Council in these instances.

The school will keep a record of all staff and pupils who are granted Internet access, i.e. through the Responsible Use agreement for pupils (Appendix 1 and covering letter to parents Appendix 2) and the staff policy for Responsible Use (Appendix 3). The record will be kept up-to-date; for instance a member of staff may leave or a pupil's access be withdrawn.

Longford Primary School's 'home-school agreement' will include the Responsible internet Use Policy and guidance for sound, image and video for publication online.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible.

Pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.

Parents will be informed that pupils will be provided with supervised Internet access.

2.2 Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

- A log of any staff with unfiltered access to the Internet will be kept and regularly reviewed.
- The school will work in partnership with parents, Wiltshire Council, DFE and its ISP to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the IT subject leader.
- Website logs will be regularly sampled and monitored by SWGfL monitoring service: <http://monitoring.swgfl.org.uk>
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e. Head teacher, LA, Police, Internet Watch Foundation. (IWF – <http://www.iwf.org.uk>)

2.3 Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.

The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored. Methods to identify, assess and minimise risks will be reviewed regularly.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

2.4 Managing content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the South West Grid for Learning: 0845 307 7870 or email: abuse@swgfl.org.uk
- Specific lessons will be included within the curriculum that teaches all pupils how to develop their media literacy skills, in particular validity and bias.
- At Key Stage 2, Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Training will be available to staff in the evaluation of web materials and methods of developing students' critical attitudes.

2.5 The use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents 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 / made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

3. Teaching and Learning

3.1 The Curriculum

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.
- The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

3.2 Enhancing Teaching and Learning

Benefits of using the Internet in education include:

- Access to a variety of worldwide educational resources.
- Inclusion in the National Education Network which connects all UK schools.
- Educational and cultural exchanges between pupils worldwide.
- 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 automatic system updates.
- Access to learning wherever and whenever convenient.

3.3 Evaluating Content

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- If staff or pupils discover unsuitable site or content they consider to be inappropriate, the URL (address) and content should be reported to the ISP/SWGfL
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

4. Communication and Content

4.1 Website Content

Many schools have excellent websites that inspire pupils to publish work of a high standard. Publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information may be better published in the school handbook or on a secure online area which requires authentication. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully and will not enable individuals to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

4.2 Managing e-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures. Only whole class or group emails will be used for and by pupils at Longford Primary School.

To keep them safe pupils must:

- immediately tell a responsible adult if they receive offensive e-mail.
- use email in an acceptable way. Sending images without consent, explicit images, messages that cause distress and harassment to others are considered significant breaches of school policy and will be dealt with accordingly.

To keep pupils safe staff must:

- only use official school provided email accounts for all professional communications.
- ensure that any E-mail sent to an external organisation is written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.

4.3 On-line communications and Social Media.

On-line communications, social networking and social media services may be filtered in school by their ISP but are likely to be accessible from home.

All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with pupils or personally. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. As a school we acknowledge the key role we have to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

- Pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.
- Staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Headteacher before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and only operate with approval from the Headteacher.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
- Parents wishing to photograph or video at an event should be made aware of the schools expectations and be required to comply with the school's Responsible Use policy as a condition of permission to photograph or record.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning a pupil's underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Responsible Use Policy.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.

4.4 Mobile Devices (Including Bring You Own Device-BYOD)

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

Mobile devices can be used to facilitate communication in a variety of ways with text, images, sound and internet accesses all common features. Mobile devices (as listed above) are not permitted in school, unless specifically requested by the teacher to support classroom learning. Clear rules and guidelines will be given to parents and pupils if such a request is made. Any mobile device brought into school must be handed to the class teacher at the start of the day.

Please note the following:

- Mobile devices that are brought in to school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- School staff authorised by the Head teacher may search pupils or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that

the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.

- Sending abusive or inappropriate messages or content is forbidden by any user within the school community.
- Mobile devices may be used during lessons or formal school time as part of approved and directed curriculum based activity.
- Mobile devices are not permitted to be used in certain areas or situations within the school site e.g. changing rooms or toilets, situations of emotional distress etc.
- Where staff may need to contact children, young people and their families within or outside of the school in a professional capacity, they should only do so via an approved school account (e.g. e-mail, phone and social media). In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to the Headteacher ASAP.
- Staff will be provided with school equipment for the taking photos or videos of pupils linked to an educational intention. In exceptional circumstances staff may need to use personal devices for such a purpose and when doing so, should ensure they comply with the school's Responsible Use Agreement.
- For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's device.
- Pupils may not be protected from inappropriate material, bullying and harassment if using their own devices in school.
- The school will take steps to monitor responsible use in accordance with the Responsible Use Policy.

4.5 Video Conferencing

Video conferencing (including FaceTime, Skype and Lync) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible should take place using the school's wireless system.

- Staff must refer to any Responsible Use agreements prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised appropriately for the pupil's age and ability.

4.6 Emerging Technologies

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 should be completed on each new technology and assessed for effective and safe practice in classroom use. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4.7 Cyber Bullying

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007.

For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that pupils, staff, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect

people and how to respond and combat misuse. We endeavour to promote a culture of confident users that will support innovation and safety.

Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's behaviour, anti-bullying and child protection policies. These include:

- Clear procedures set out to investigate incidents or allegations of cyber bullying.
- Clear procedures in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos.

4.8 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Schools will already have information about their obligations under the Act; this section is a reminder that all data from which people can be identified is protected. For advice and guidance relating to a contravention of the Act, contact www.wiltshire.gov.uk

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

5 Implementation

5.1 Policy in Practice - Pupils

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of the school's e-safety teaching and awareness-raising it is important to discuss the key features with pupils as appropriate for their age. Pupils may need to be reminded of the school rules at the point of Internet use.

- All users will be informed that network and Internet use will be monitored.
- Online Safety teaching is integral to the curriculum and we will raise the awareness and importance of safe and responsible internet use amongst pupils.
- Online Safety teaching will be included in PSHE, Citizenship and/or Computing and cover safe use at school and home.
- Online safety will be taught at the beginning of each academic year, before any internet use.
- Online Safety rules and/or copies of the Responsible Use Policy will be on display in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

5.2 Policy in Practice - Staff

It is important that all staff feel confident to use new technologies in teaching and the School Online Safety Policy will only be effective if all staff subscribe to its values and methods. Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies.

Where staff are provided with devices by the school which may be accessed outside the school network they are bound by this Online Safety Policy. Inappropriate materials, images and websites must not be accessed or stored on school equipment. Staff are responsible for maintaining confidentiality of school information. If a member of staff is concerned about any aspect of their COMPUTING or internet use either on or off site, they should discuss this with the Headteacher to avoid any possible misunderstanding.

- The Online Safety Policy is provided to and discussed with all members of staff and Responsible User Policy signed for compliance.
- Staff will be made aware that Internet traffic is monitored (and automatically reported by the SWGfL) and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

5.3 Policy in Practice - Parents

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.

- Parents' attention will be drawn to the Online Safety Policy and Responsible User Policy RUP in newsletters, school prospectus and Website.
- A partnership approach with parents will be encouraged. This may include parent evenings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

5.4 Handling of complaints

Parents and teachers must know how and where to report incidents in line with the school complaints policy and complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures. Prompt action will be required if a complaint is made. The facts of the case will need to be established; for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All records of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc.

- Responsibility for handling incidents will be delegated to the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Refer to Appendix 4 for 'Responding to Incidents of Misuse' flowchart.



Rules for Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including

- access to web-sites
- the interception of e-mail
- the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place
- detecting if the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

The South West Grid for Learning (SWGfL) monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.

Appendix 2

Longford C of E Primary School
Admin Office
High Road
Britford
Salisbury SP5 4DS



Dear Parents/Guardians,

Responsible Use of the Internet

As part of your child's curriculum and the development of computing skills, Longford Primary School provides supervised access to the internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Our internet access is provided by 'Schools Broadband' and operates a filtering system to restrict computing access to inappropriate materials. All of our laptops, iPads and screens will be in public view and an adult is present to supervise.

No system is perfect, however. You should be aware that it is not possible to remove entirely the risk of finding unsuitable material. The school cannot be held responsible for the nature and content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the internet.

We have clear rules that the children are expected to follow to help with the precautions we have put in place. Children benefit enormously from this facility and use it responsibly. I would ask that you look through these rules and discuss them with your child. Then return the signed form to us at the school by

Yours sincerely,

Louise Knipe
Headteacher

Continued...

Pupil:

Class:

Pupil's Agreement

I have read and I understand the school rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

Signed:

Date:

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:

Date:

Please print name:

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the school Website. I also agree that images, sound files and video that include my son/daughter may be published subject to the school rules that this content will not clearly identify individuals and that full names will not be used.

Signed:

Date:

Please print name:

Appendix 3

Responsible User Policy

Longford CofE Primary School recognises the important contribution and value technology can play in promoting students' learning and development, however, there are potential risks involved. We have rigorous online safety policy and procedures in place and have taken positive steps to reduce this risk in school as we believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.

Allowing the use of mobile devices is a school decision, and should be subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Users have access to resources to support learning and teaching
- Users should be given clear boundaries on responsible and professional use

Access to network services is given to users who act in a considerate, appropriate and responsible manner. Users are responsible for their behaviour on school networks just as they are in any part of the school. Access is a privilege—not a right—and entails responsibility. We expect all users to use technology, both that belonging to the school or their own, responsibly and safely according to the following conditions:

For the purposes of this document, technology means any device that provides a connection to the Internet or internal network.

1. A device loaned to you by the school for an education related purpose remains the property of Longford CofE Primary School.
2. Only approved user devices may connect to the school network by prior agreement.
3. A device must remain in your possession, should only be used by you and should be securely stored when not in use.
4. Longford CofE Primary School policies regarding the appropriate use and sharing information apply to devices both school and privately owned. Use of any device must adhere to data protection, online safety and health and safety rules.
5. Devices may be used for education related purposes at the discretion and under the supervision of the teacher or responsible adult.
6. If used to create or store personal information including images and videos of pupils, users must fully comply with high standards of data protection as set out in the Data Protection Act 1998.
7. A device connecting to the school network may be configured with certain restrictions in place. Any settings that are passcode protected must not be changed.
8. Insurance cover provides protection for school owned devices from the standard risks whilst the device is on site or in your home **but excludes** theft from a car or other establishment. Should the device be left unattended and is stolen, you will be responsible for its replacement.
9. Privately owned devices remain the responsibility of the owner and will not be covered under the school insurance policy.
10. All devices whether owned by the school or privately owned, may be subject to regular checks for compliance with school policies. Failure to comply or evidence of unacceptable use will result in sanctions or disciplinary action.

Unacceptable use includes but is not limited to:

- Make, store, post, download, upload or pass on, material, remarks or images that may be offensive or upsetting to an individual or group;
- Make, store, post, download, upload or pass on images of individuals without their permission (or in the case of images of pupils, the permission of their parent or carer);

- Giving personal information, such as complete name, phone number, address or identifiable photo, without permission from teacher and parent or guardian;
- Using obscene language;
- Damaging or modifying computers, computer systems or computer networks: downloading, installing and using games, audio files, video files or other applications including shareware or freeware without permission to do so;
- Violating copyright laws ;
- Sharing or using others' logons or passwords or other confidential information;
- Trespassing in others' folders, work or files;
- Intentionally wasting limited resources;
- Employing the network for non-academic, personal, commercial, political purposes, financial gain, or fraud;
- Attaching unauthorised equipment to the school network.

Approved Devices.....

Authorised by Date

Name

I/we have read this agreement and fully understand that I/we need to adhere to all elements

User signature Date.....

Parent / Guardian signature Date.....

Please notify the school of any changes or additions to this list of approved devices.

You are reminded that you are always subjected to the Data Protection Act 1998, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.

Responding to incidents of misuse – flow chart

