
Longleaze Primary School Online Safety Policy - December 2017

Longleaze Primary School Online Safety Policy



1. Leadership and Management

1.1 Who will write and review our policy?

- Our Online Safety policy has been written by the school, building on the Wiltshire e-safety template policy and government guidance. It has been created with input from children, staff, parents and governors. It has been agreed by the Senior Management team and approved by governors. It will be reviewed annually.

It relates to other policies, for example Behaviour, Anti-Bullying, PSHE, Child Protection, Safeguarding and Staff Code of Conduct for Safer Working Practice.

Created by: Martin Yeo

Date: May 2017

To be reviewed: April 2018

Approved by:

1.2 How will internet access be authorised?

Internet access for children should be seen as an entitlement on the basis of educational need to enhance learning and is an essential resource to support teaching and learning. Parental permission for children to use the internet at an age appropriate level will be sought on entry to Reception class or when a child joins the school. SWGfL proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred and radicalisation) content and will notify the local police and Wiltshire Council in these instances.

- *The Longleaze 'Home School Agreement' will include the Responsible Use Policy and guidance for sound, image and video for publication online. Parents/carers will sign this when children join the school, to confirm their understanding of our school's policy on responsible internet use.*
- *Longleaze School's Internet access will be designed expressly for children's use and will include filtering appropriate to the age of the children.*
- *In the Early Years' Foundation Stage, access to the internet is likely to be by adult demonstration only. In Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.*
- *At Key Stage 2, children will be able to search the internet independently, using child-friendly, approved search engines, with the children being taught appropriate keywords with which to*

search. The children will be supervised at all times. Children will be taught what to do if they come across unsuitable and inappropriate materials so that these skills are embedded by the time they are using the internet independently.

- *Parents will be informed that children will always be provided with supervised Internet access in school.*
- *All devices in school will access internet through secure and filtered Wifi. The School's internet connection is filtered and secure.*

1.3 How will filtering be managed?

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 child's age and experience. Internet access must be appropriate for all members of the school community from the youngest child to the oldest and all members of staff.

- *A designated member of staff will review the popular permitted and banned sites accessed by the school.*
- *The school will work in partnership with parents, Wiltshire Council, DFE and its ISP to ensure systems to protect children are reviewed and improved.*
- *If staff or children discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the Online Safety lead.*
- *Website logs will be regularly sampled and monitored.*
- *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 will be referred to the appropriate authorities i.e. Head teacher, Safeguarding Lead, LADO, Police, CEOP or Internet Watch.*

1.4 How will the risks be assessed?

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 children 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 children. 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.*
- *Methods to identify, assess and minimise risks will be reviewed regularly.*
- *The Head Teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.*
- *The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.*

2. Teaching and Learning

2.1 Why is Internet use important?

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires children 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 the use of technology is now seen as an essential life-skill.

- *Internet use is a part of the statutory curriculum and a necessary tool for staff and children.*
- *The purpose of Internet use in school is to raise educational standards, to communicate, promote children's 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. Children are expected to agree to the Responsible Use policy.*
- *The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience.*
- *Children 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.*

2.2 How will Internet use enhance learning in our School?

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 children worldwide.*
- *Vocational, social and leisure use in libraries, clubs and at home.*
- *Access to experts in many fields for children 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.*

2.3 How will children learn to evaluate Internet content?

Information received via the web, including e-mail and other forms of communication 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 children using the web but this is not easy to achieve and cannot be guaranteed. Children should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- *Children will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.*
- *Children 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. The South West Grid for Learning Digital Literacy curriculum will provide enriching opportunities for children to take greater responsibility for their behaviour online.*
- *If staff or children discover unsuitable sites or content they consider inappropriate, the URL (address) and content must be reported to South West Grid for Learning.*
- *The school will ensure that the use of Internet derived materials by staff and by children complies with copyright law.*
- *Children will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.*

3. Communication and Content

3.1 How will the School's Website be managed?

Publication of any information online will always be considered from a personal and school security viewpoint. Sensitive information will be published in the school prospectus or on a secure online area which requires authentication. Where children's work is published, editorial guidance will help reflect the school's requirements for accuracy and good presentation.

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

3.2 How will email communication be managed?

E-mail is an essential means of communication for both staff and children. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

We will determine the best approach for using email with the children, based upon children's age and curriculum requirements. The use of email identities using children's names such as john.smith@school.wilts.sch.uk will be avoided as revealing this information could potentially expose a child to identification by unsuitable people.

- *Children may only use approved e-mail accounts on the school system to send email internally.*
- *Children must immediately tell a responsible adult if they receive offensive e-mail.*
- *Children should use email in an Responsible way. Sending images without consent, explicit images, messages that cause distress and harassment to others are considered significant breaches of school RUP and will be dealt with accordingly.*
- *E-mails sent externally will be sent only when forwarded via the class teacher.*
- *The Senior Leadership Team will monitor the school email account to ensure only appropriate communications are sent.*
- *Staff must use official school provided email accounts for all professional communications.*
- *In order to avoid the risk of the school's network being infected by viruses or malicious software e.g. Ransomware, staff members will be vigilant when opening emails, not opening emails that appear suspicious e.g. from unknown senders.*
- *Staff must not use official school provided email accounts for their own private communications.*
- *When sending emails, children's names must not be used but indicated by initials only.*
- *Any document attachments which pertain to children must be encrypted before sending.*
- *Any portable devices that are linked to school email laptop/IPADs must be password protected.*

3.3 How will online communication and social media be managed in school?

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

All staff will be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. Staff will be made aware of the importance of considering the material they post and the possible impact on the school community. Staff must ensure profiles are secured and recognise how publishing unsuitable material may affect their professional status. Social Media policy (April 2016) for further guidance.

Children will 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. We recognise that we, as a school, have a key role to teach children about the importance of keeping personal information safe.

- *Children 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.*
- *Children must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or arrange to meet anyone.*
- *Children 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.*

- *Children will be taught responsible personal publishing through age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.*
- *Children will be taught the importance of approving and inviting only known friends and to deny access to others by making profiles private. They will be taught how to block and report all unwanted communications.*
- *All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.*
- *Staff official blogs kept for educational purposes will be password protected and only operate with approval from the SLT.*
- *Concerns regarding the vulnerability of children who are at risk of radicalisation and extremism will be shared with the Safeguarding Lead, Head Teacher, Multi-Agency Safeguarding Hub (MASH Team) or the Police, as appropriate.*
- *Concerns regarding children's 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 children's underage use of sites. This will include access to materials viewed via DVD or video games, as well as online.*
- *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's Responsible Use Policy.*
- *In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it is unacceptable for staff to engage in personal online communications with children and young people, parents or carers, using personal e-mails addresses, in regard to school matters. Express care is also to be taken regarding the use of social networking sites. (See Social Media Policy 2016).*
- *Parents wishing to photograph or video at an event, either in school or off-site at a school related event, must not post images captured to the Internet, in compliance with the school's Responsible Use Policy.*
- *Parents are asked to carefully consider, before posting content on social media sites, whether it is appropriate to post certain content or if to do so would bring the school into disrepute, breach confidentiality or copyright or if it could be considered offensive, defamatory, discriminatory, bullying or is potential harassment to an individual employed by the school. Where incidents of this nature are brought to the attention of the Senior Leadership Team, and they are deemed to be defamatory in some way, you will be invited into school to discuss the matter further and we may request that you remove the post or we may report abuse to the site involved.*

3.4 How will mobile phones and personal mobile devices be managed?

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 phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet access all common features. A policy which prohibits users from taking mobile devices to school could be considered to be unreasonable and unrealistic for

schools to achieve. Due to the widespread use of mobile devices it is essential that schools take steps to ensure that these devices, both personally and school owned, are used responsibly and that they do not impede teaching and learning. Staff will be given clear boundaries on professional use.

The use of mobile phones and personal devices is a school decision, and is subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Children and staff have access to resources to support learning and teaching
- Our school community will be given clear boundaries on responsible and professional use

These principles underpin our policy, which states that:

- *Sending abusive or inappropriate messages or content is forbidden by any user within the school community.*

Policy for children

- *Mobile phones that are brought in to school by children will be stored in the School Office during the school day. However, they remain the responsibility of the user and the school accepts no responsibility for the loss, theft or damage of such items.*
- *Children must not take mobile phones on school trips or residential visits.*
- *School staff authorised by the Head teacher may search children 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.*

Policy for staff and visitors

- *Mobile phones that are brought into school by any member of staff or visitors must be stored remotely, away from the classrooms. Lockers are available for this purpose or they may be stored in the School Office during the school day. However, the school accepts no responsibility for the loss, theft or damage of such items.*
- *Staff mobiles will be turned off during teaching time and turned to silent during any staff or school led meeting.*
- *Personal electronic devices provided by the school may be used during lessons or formal school time as part of approved and directed curriculum based activity.*
- *Where staff may need to contact children and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail or phone), unless under the direction of the headteacher e.g. residential. In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.*
- *During school hours, where family members may need to contact staff in an emergency situation, they should telephone the School Office in the first instance. Only in **exceptional** circumstances, and in agreement with the Head Teacher, will a member of staff be allowed to use a mobile phone during learning time.*

- *Staff will be provided with school equipment for the taking of photos or videos of children for educational purposes and will only use work-provided equipment for this purpose.*
- *Wherever possible, contractors will be asked to carry out maintenance outside of school hours. Where essential maintenance or emergency repair is required in teaching areas during school hours, all contractors will be supervised to comply with this policy.*
- *For the safeguarding of all involved, users must 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.*
- *The school will take steps to monitor responsible use in accordance with the Responsible Use Policy*
- *A school mobile phone will be passcode protected and given to the designated Trip Leader to ensure confidentiality of mobile records.*

3.5 How will we ensure emerging technology is used safely?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, video conferencing, Internet access, collaboration and multimedia tools. A risk assessment will be completed on each new technology and assessed for effective and safe practice in classroom use.

- *Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The risk assessment will be evaluated by a member of the SLT.*

3.6 How will we teach children about cyber-bullying?

Many children and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that children, school staff and parents/carers understand how cyber-bullying is different from other forms of bullying. It is important to understand how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety within our school.

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. Examples of how cyberbullying may occur include via mobile phones, social networking sites, gaming, forums, email and sexting. The DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyber-bullying: <http://www.digizen.org/cyberbullying>.

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 Anti-bullying and Child Protection policies, which include:

- *Clear procedures are in place to investigate incidents or allegations of cyber bullying.*
- *Clear procedures are 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 and investigated by the designated Safeguarding Lead.*
- *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 service provider and the police, if necessary.*

- *Children, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's online safety ethos.*

3.7 Data Protection

The quantity and variety of data held on children, 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, which provides guidance for schools.

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

4 Implementation

4.1 Introducing the Policy to Children

Many children are very familiar with Internet use and the culture that surrounds it. As part of the school's online safety teaching and awareness-raising it is important to discuss the key features with children as appropriate for their age. Children 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 will be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst children.*
- *Appropriate staff training will be completed annually.*
- *Online Safety teaching will be included in the curriculum and cover safe use at school and home.*
- *Online Safety rules will be on display in all classrooms and learning spaces with Internet access. A copy of the Responsible Use Policy will be available in the School Office.*
- *The SWGFL digital literacy curriculum scheme of work will be established across the school to raise awareness and importance of safety and responsible internet use amongst children.*
- *Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.*

4.2 Consultation with Staff on the Policy

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

All staff must understand that the rules for information systems misuse for Wiltshire Council employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

- *The Online Safety Policy will be provided to and discussed with all members of staff and the Responsible Use Policy signed for compliance.*
- *Staff will be made aware that Internet traffic is monitored (and automatically reported by 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.*

4.3 How will we share Online Safety with 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. Schools may wish to refer parents to websites referred to in the references section of this document.

- *Parents' attention will be drawn to the Online Safety Policy and Responsible User Policy in newsletters, school prospectus and website.*
- *A partnership approach with parents and carers will be encouraged. This will include offering annual Online Safety updates alongside your children, as well as offering practical advice and resources to support safer Internet use at 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.*
- *Parents will be informed if the School become aware of any children showing evidence of inappropriate use of the Internet at home.*
- *Regular information will be provided to parents about how to ensure they can work with the school to ensure online safety is practised responsibly, both within school and at home.*

4.4 How will complaints be handled?

Parents and teachers must know how and where to report incidents in line with the school complaints policy. 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. All records of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc. Complaints of a child protection nature will be dealt with in accordance with the Local Authority's Child Protection procedures.

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

Longleaze Primary School

December 2017

Rules for Responsible Internet and Device Use for Adults



1. I will use all ICT equipment issued to me in an appropriate way, in line with the Online Safety policy and the Social Media Policy. I will not:
 - Access offensive website or download offensive material.
 - Make excessive personal use of the Internet or e-mail.
 - Copy information from the Internet that is copyright or without the owner's permission.
 - Place inappropriate material, or that which may impact negatively on the School community, onto the Internet.
 - Send e-mails that are offensive or otherwise inappropriate.
 - Disregard my responsibilities for security and confidentiality with regard to children's identities and data protection.
 - Download files that will adversely affect the security of the laptop/IPAD and school network.
 - Update web pages or use pictures or text that can identify the school and individual children.
 - Attempt to repair or interfere with the components, software or peripherals of any IT equipment that is the property of Longleaze Primary School.
2. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
3. When emails relate to children within the school, I will encrypt any attachments sent and ensure that only initials are used for identification.
4. Any removable media I use will be encrypted and free from any type of virus.
5. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Online Safety Lead or IT technician.
6. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
7. I will report immediately to the Headteacher or Online Safety Lead any unpleasant material or messages sent to me.
8. I understand that consequences will be taken if I deliberately access Internet sites that contain certain illegal material.
9. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
10. Activity that threatens the integrity of the school IT systems, or activity that attacks or corrupts other systems, is forbidden.
11. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop/IPAD removed and that other disciplinary consequences may follow.
12. I agree to follow the Online Safety and Social Media policy, in relation to the recreational use of social networking sites or other online technologies.
13. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the Headteacher and register the passwords with the Headteacher.
14. I will ensure I keep my network password secure and inform the Office Manager if this security is breached.

Signed:

Date:

Longleaze Primary School

May 2017

Rules for Responsible Internet Use for Children



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

- I will ask permission before using the Internet and will only use the internet if there is an adult close by to supervise me.
- 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 or use software or files from home.
- I understand that any mobile devices that I bring into school will be stored in the School Office.
- I will only e-mail and open attachments from people I know, or my teacher has approved, through the school system.
- Any messages I send will be polite and sensible.
- I understand that I must never post my home address, phone number or email address online, or arrange to meet someone.
- I will not use the Internet in school to access social media sites.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell an adult immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit and there may be consequences if anything inappropriate is found.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers and that my parents/carers may be informed.

I have read and 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: April, 2016

Dear Parents and Carers

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Longleaze Primary School provides supervised access to the Internet. We believe that the effective use of the Internet and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Although there are concerns about children having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, the South West Grid for Learning (SWGfL) operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or 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 facilities.

We have recently updated our Online Safety Policy, which is available for you to view in the School Office, if you wish to have clarity on how the internet is accessed as your child moves through the School. Should you wish to discuss any aspect of Internet use in our School, please contact the Office for an appointment.

Yours sincerely

Laura Oakes
Head Teacher

**Longleaze Primary School
Responsible Internet Use**

Please complete, sign and return to the School Office.

Child:

Class:

Child'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:

Parental 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 children 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:

Parental 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:

Parental consent form for use of children’s media

At Longleaze School we take the issue of child safety very seriously, and this includes the use of images / sound files and video of children. Including images of children in school publications and on the school website can be motivating for the children involved, and provide a good opportunity to promote the work of the school. However, schools have a duty of care towards children, which means that children must remain unidentifiable, reducing the risk of inappropriate contact, if images are used in this way.

We ask that parents and carers consent to the school taking and using photographs and images of their children. Any use of children’s images at Longleaze Primary School is underpinned by our Online Safety policy. We will never include the full name of the child alongside an image.

Please complete, sign and return this form to the office at Longleaze Primary School.

I consent to photographs and digital media of the child named below, appearing in Longleaze Primary School printed publications or on the school website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed by other media, such as CD-ROM, as part of the promotional activities of the school.

Name of child:

Name of parent or carer:

Address:

.....

.....

Signature:

Date:

Queries regarding this form should be addressed to the Headteacher or Online Safety Lead at Longleaze Primary School.

Staff Professional Conduct Agreement

Laptop/IPAD policy for Longleaze School staff

1. The laptop/IPAD remains the property of Longleaze School.
2. The laptop/IPAD is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Longleaze School Staff should use the laptop/IPAD.
3. On the teacher leaving the school's employment, the laptop/IPAD must be returned to Longleaze School on the last day of the term in which they leave.. Staff on extended leave of 4 weeks and over should return their laptop/IPADS to the school (other than by prior agreement with the Headteacher).
4. When in school and not being used, the laptop/IPAD must be kept in a safe place. It must not be left in an unlocked, unattended classroom.
5. Laptops and IPADS must not be left in an unattended car, due to the confidential nature of the data therein. In exceptional circumstances, if there is a need to do so, it should be locked in the boot.
6. The laptop/IPAD must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Headteacher, with evidence of adequate insurance.
7. All software on laptops and IPADS must be fully licensed and have been installed by our IT technician, to ensure that no corrupt software or systems are installed.
8. If any removable media is used, then it must be encrypted and checked to ensure it is free from any viruses.
9. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop/IPAD is kept up-to-date.
10. Staff must use their laptop/IPAD in school on the network at least once a week to ensure virus protection is automatically updated.
11. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
12. Staff should communicate with the School's IT technician with regard to technical issues, or the need to modify the laptops/IPADS.
13. Students can only use the laptop/IPAD under the direct supervision of an adult.
14. If any fault occurs with the laptop/IPAD, it should be referred immediately to the IT Technician.
15. The laptop/IPAD would be covered by normal household insurance. If not it should be kept in school and locked up overnight.
16. The purchase and installation of Apps on school IPADS must be agreed and carried out by appropriately authorised members of staff (IT Technician, Office Manager).

The device I have is(serial no.). I agree to adhere to this Conduct Agreement.

Signed:

Date:

Web-based Resources

For Schools

KidSmart

<http://www.kidsmart.org.uk/>

SMART rules from Childnet International and Know It All for Parents

Childnet International

<http://www.childnet-int.org/>

Guidance for parents, schools and children

Thinkuknow

<http://thinkuknow.co.uk>

Child friendly Online Safety resources

Internet Watch Foundation

www.iwf.org.uk

Invites users to report illegal Websites

South West Grid for Learning – Safe

www.swgfl.org.uk/safe

A comprehensive overview of web-based resources to support schools, parents and children

South West Grid for Learning – Filtering

<http://www.swgfl.org.uk/services/default.asp?page=filtering>

For Parents

Kids Smart

<http://www.kidsmart.org.uk/parents/advice.aspx>

A downloadable PowerPoint presentation for parents

Childnet International

<http://www.childnet-int.org/>

“Know It All” CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online.

<http://www.bbc.co.uk/webwise/>

<http://www.iwf.org.uk/>

<http://www.getnetwise.org/>

Useful contact details:

South West Grid for Learning (SWGfL) Support Team - (including the registering of inappropriate content needing to be filtered).

Telephone: **0870 9081708**

E-mail: **support@swgfl.org.uk**

To notify of an inappropriate website: **abuse@swgfl.org.uk**