Winsor Primary School
Online Safety Policy

Drafted By:	**Louise Hepple (Deputy Head Teacher)**
Date:	**September 2017**
Ratified by Governors:	**12th October 2017**
Review Date:	**October 2018**

Policy Statement

For clarity, the online safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school, e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips, etc.

Wider school community – students, all staff, governing body, parents *and visitors*

Safeguarding is a serious matter; at Winsor Primary we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as online safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Winsor Primary website; upon review all members of staff will sign as read and understood both the Online Safety Policy and the Staff Acceptable Use Policy. A copy of this policy and the Students' Acceptable Use agreement will be shared with students at the beginning of each school year. Children are asked to sign to say they agree with the rules.

Roles & Responsibilities

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of online safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Head Teacher in regards to training, identified risks and any incidents.
    - Chair the Online Safety Committee

Head Teacher

Reporting to the governing body, the Head Teacher has overall responsibility for online safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Officer (or more than one), as indicated below.

The Head Teacher will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated Online Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All online safety incidents are dealt with promptly and appropriately.

Online safety Officer

The day-to-day duty of Online Safety Officer is devolved to *Renee Saul and Louise Hepple*
The Online Safety Officers will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.

- Review this policy regularly and bring any matters to the attention of the Head Teacher.
- Advise the Head Teacher, governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail. Monitor Impero for any inappropriate activity.
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Head Teacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any online safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and Head Teacher.
    - Passwords are applied correctly to all users regardless of age.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head Teacher.
- Any online safety incident is reported to the Online Safety Officer via Safeguard Software (and an Online Safety Incident report is made by Learning Mentors), or in his/her absence to the Head Teacher. If you are unsure the matter is to be raised with the Online Safety Officer or the Head Teacher to make a decision.
- The reporting flowcharts contained within this Online Safety Policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour Policy.

Online Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and workshops the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Winsor Primary uses a range of devices including PC's, laptops, Ipads etc. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

- SafeMail, our pupils' email system, is secured so it's only possible to send and receive emails between people and groups within your school
- URL filtering platform helps protect pupils from accessing inappropriate websites
- Using the LGfL, our schools' broadband connection links to many educational resources and services without accessing the wider internet
- Impero Education Pro software helps to keep distractions and unsuitable content at bay. At the click of a button, teachers can lock screens to focus learning or remote control any student device to solve issues. A live thumbnail view of all devices means student activity can be closely monitored on-the-fly, while real-time violation alerts help teachers to keep students focused and safe. This, along

with keyword detection, including built-in abuse libraries, identifies students at potential risk, so primary schools can provide the appropriate support.

Passwords – all staff and students will be unable to access any device without a unique username and password. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed where necessary.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Head Teacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this online safety and the Staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Winsor Primary is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. Social media services used in school have to be appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Online Safety Officer who will advise the Head Teacher for a decision to be made. Any new service will be risk assessed before use is permitted.

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any online safety incident is to be brought to the immediate attention of the Online Safety Officer, or in his/her absence the Head Teacher. The Online Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Winsor Primary will have an annual programme of training which is suitable to the audience.

Online Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The Online Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head Teacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head Teacher for further CPD.

The Online Safety Training Programme can be made available by the Online Safety Officer.

Monitoring and Filtering

Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the online safety toolbox that is of particular importance. When talking about an Internet filter there are two important aspects:

Very broadly speaking

- **Filtering** - this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.
- **Monitoring** - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

Why do we Filter and Monitor?

Schools filter Internet activity for two reasons:

We filter to ensure

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance

- (as much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

All staff, students and parents of students will be informed that Internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites.

How to deal with online safety incidents – indicative sanctions for pupils and/or staff:

Illegal activities:

- The Head Teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter.

- The Police and IWF/CEOP should be contacted. Child Protection procedures take precedence over AUPs if CP is a factor.
- The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.

Going on the Internet in lessons or using websites not relevant to the lesson in lesson time:

- Pupil: The class teacher or form tutor will deal with the matter and write up an incident report to submit to the Online Safety Officer.
- Staff: the issue may be raised by SLT to the Head Teacher as a disciplinary matter.
- Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the Online Safety Officer.
  Staff: the issue may be raised by SLT to the Head Teacher as a disciplinary matter.
- The person will receive a warning.

Bypassing the school's filtering system:

- Pupil: The class teacher will deal with the matter and write up an incident report to submit to the Online Safety Officer.
- Staff: The issue may be raised by SLT to the Head Teacher as a disciplinary matter.
- The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.
- Additionally, parents or guardians will need to be informed.
- The person involved will lose access to the network and/or Internet as per the AUP agreement.

Viewing pornographic material:

- Pupil: The Safeguarding and Pastoral Manager will deal with the matter and write up an incident report to submit to the Online Safety Officer.
- Staff: the issue will be raised by SLT to the Head Teacher as a disciplinary matter.
- The Police and IWF should be contacted if indecent material was uploaded or downloaded. CEOP should be contacted if grooming / sexting or unwanted sexual advances were involved.
- The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.
- Additionally, parents or guardians will need to be informed.
- The person involved will lose access to the network and/or Internet as per the AUP agreement.

Using a mobile phone, social media or other digital device in a lesson:

- Pupil: The class teacher will deal with the matter and write up an incident report to submit to the Online Safety Officer.

- Staff: The issue may be raised by SLT to the Head Teacher as a disciplinary matter.

Cyber bullying:

- Pupil: The class teacher will deal with the matter and write up an incident report to submit to the Online Safety Officer.
- Staff: The issue may be raised by SLT to the Head Teacher as a disciplinary matter.

Writing malicious comments about the school or bringing the school name into disrepute – whether in school time or not:

- Pupil: The class teacher will deal with the matter and write up an incident report to submit to the Online Safety Officer.
- Staff: The issue may be raised by SLT to the Head Teacher as a disciplinary matter.

Trying to hack or hacking into another person's account, school databases, school website, school emails or online fraud using the school network:

- Depending on the severity of the incidence, the cybercrime unit, www.actionfraud.police.uk/ or local police could be contacted.

Online Safety and the Law:

Computer Misuse Act 1990, sections 1-3
Data Protection Act 1998
Freedom of Information Act 2000
Communications Act 2003 section 1,2
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988
Racial and Religious Hatred Act 2006
Protection of Children Act 1978
Sexual Offences Act 2003
The Education and Inspections Act 2006 (Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the school behaviour policy.)

Useful links to external organisations:

Ofsted:

- www.gov.uk/government/publications/school-inspection-handbook

DfE:

- www.gov.uk/government/groups/uk-council-for-child-Internet-safety-ukccis

CEOP:

- www.ceop.police.uk/safety-centre/
- childnet-int.org/

UK Safer Internet Centre:

- www.saferInternet.org.uk/safer-Internet-day

- www.saferInternet.org.uk/

Internet Watch Foundation:

- www.iwf.org.uk
- www.iwf.org.uk/members/get-involved

Links to training:

Online safety Support: online refresher training www.online safetysupport.com/online_training

CEOP: www.ceop.police.uk/training/

NAACE: online safety online training: www.naace.co.uk/ictcpd4free

EPICT: offline and online online safety training: www.epict.co.uk/#!esafetyinfo/cq8q

Movies and presentations:

www.swgfl.org.uk/Staying-Safe/online safety-Movies

www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware

Other publications:

- Safer children in a digital world: the report of the Byron Review (PP/D16(7578)/03/08), DCSF and DCMS, 2008; http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/byronreview/.
- Ofcom's response to the Byron Review, Ofcom, 2008; http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/byron/.

Appendix 1

Winsor Primary School Computer and Internet Acceptable Use Policy

For Staff

All staff having access to the networks must sign a copy of this Computer and Internet Acceptable Use Policy and return it to the School Office.

The computer network is owned by the school and is made available to staff to assist their professional development. This computer and Internet Acceptable Use Policy covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems and has been drawn up to protect everyone.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the school's approved, secure email system(s) for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to Louise Hepple, Online Safety Lead or Renee Saul, Computing Co-ordinator
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to Renee Saul or Louise Hepple on request.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's Data Protection procedures.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended system.
- I will not use personal digital cameras or camera phones for transferring images of pupils or staff without permission.
- I will use the MLE in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and are secure against access by uninvited users i.e. students both current and former.

- I will not engage in any online activity that may compromise my professional responsibilities.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely for professional use.
- I will ensure any confidential data that I wish to transport from one location to another is password protected.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will ensure I am aware of digital safety-guarding procedures so they are appropriately embedded in my classroom practice.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the online safety/ Safeguarding/Child Protection Lead.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

ALL SCHOOL NETWORK, INTERNET AND MANAGED LEARNING ENVIRONMENT SYSTEMS ARE MONITORED AND WE RESERVE THE RIGHT TO EXAMINE ANY AREA OF THESE SYSTEMS.

The use of computer systems without permission or for inappropriate purposes could be a criminal offence under the Computer Misuse Act 1990 (The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).)

User Signature

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

I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

I am aware that, for security, school Ipads and phones will be tracked and therefore may disclose my location.

Signature .....Date.....

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature (Head Teacher/Deputy Head/ Assistant Head)

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

Appendix 2

Winsor Primary School Computer and Internet Acceptable Use Policy – KS1

Think before you click

S 	I will only use the Internet and email with an adult
A 	I will only click on icons and links when I know they are safe
E 	I will only send friendly and polite messages
E 	If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

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

- I will ask permission before using the Internet.
- I will only look at or delete my own files.
- I understand that I must not bring software or disks into school without permission.
- I will only e-mail 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.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat, unless it through my classroom on the MLE.
- 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 the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

Pupil:	**Class:**
Pupil's Agreement: _____ **I have read and I understand the school Rules for Acceptable Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.**	

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 and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix 5

Winsor primary school Computer and Internet Acceptable Use Policy – Primary Parents

Parents online safety agreement form

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, e-mail* and other ICT facilities at school.

I know that my daughter or son has signed an online safety agreement form and that they have a copy of the 12 'rules for responsible ICT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email*, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their online safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent / guardian signature: _____

Date:__/___/___

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably

promotes the work of the school, and for no other purpose.

Parent / guardian signature: _____ Date: ___/___/___

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
  e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.

- Your child's image for presentation purposes around the school;
  e.g. in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. If used on the school website, any pictures will be of a low resolution to hinder identification. In rare events, your child's could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Parent / guardian signature: _____ Date: ___/___/___

Appendix 6

12 Rules for Responsible ICT Use – Primary

Keeping safe: stop, think, before you click!

12 rules for responsible ICT use

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

- I will only use the school's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

Appendix 7: Example Risk Assessment

Risk No.	Risk
3	In certain circumstances, students will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well-being of the child.
LIkelihood 3	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 3.
Impact 3	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
Risk Assessment	HIGH (9)
Risk Owner/s	online safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using XXXXXXXX software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same

	level of Internet filtering at home as he/she gets whilst in school. Education: The online safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school online safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.

Approved / Not Approved (circle as appropriate) **Date:**

Signed (Head Teacher) : **Signed (Governor) :**