OUGHTRINGTON
COMMUNITY
PRIMARY SCHOOL

Online Safety Policy

Oughtrington Community Primary School
Lymm
Cheshire
WA13 9EH

01925 752 086
Oughtrington_primary@warrington.gov.uk
Oughtringtoncps.co.uk

Version	Date	Action
1	March 2008	Updated Policy
2	February 2009	Updated Policy
3	February 2010	Updated Policy
4	February 2011	Updated Policy
5	March 2012	Updated Policy
6	November 2013	Updated Policy
7	September 2015	Updated Policy
8	January 2017	Changed to Online Safety

Introduction

Online Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The Schools' Online Safety Policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's Online Safety policy will operate in conjunction with other policies and Codes of Conduct.

End to End Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Exa Network including the effective management of filtering.
- National Education Network standards and specifications.

Online Safety Audit

This quick audit will help assess whether the basics of Online Safety are in place. Oughtrington Community Primary School will also design learning activities that are inherently safe and might include those detailed within Appendix 1.

The school has an Online Safety Policy that complies with Warrington guidance.	**Y/~~N~~**
Date of latest update: **January 2017**	
The Policy was agreed by governors on: **January 2017**	
The Policy is available for staff at: **School Office and School Website**	
And for parents at: **School Office and School Website**	
The Designated Safe Guarding Officer is: **Headteacher**	
The Online Safety Coordinator is: **Headteacher**	
How is Online Safety training provided? **Staff Training**	
Is the Think U Know training being considered?	**Y/N**
All staff are provided with an Acceptable ICT Use Agreement on appointment.	**Y/N**
Parents agree that their child will comply with the school Acceptable ICT Use statement.	**Y/N**
Rules for responsible use have been set for pupils:	**Y/N**
These rules are displayed in all rooms with computers.	**Y/N**
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	**Y/N**
The school filtering policy has been approved by SLT.	**Y/N**
An ICT security audit has been initiated by MGL, possibly using external expertise.	**Y/N**
School personal data is collected, stored and used according to the principles of the Data Protection Act.	**Y/N**
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT.	**Y/N**

Writing and reviewing the Online Safety Policy

- The school's Online Safety Coordinator is the Headteacher, in addition to being the Designated Safe Guarding Officer, as the roles overlap.
- Our Online Safety Policy has been written by the school, building on the Warrington Online Safety Policy and government guidance. It has been agreed by teaching staff and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why Internet use is important

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

Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be taught the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate Internet content

- Our school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems capacity and security is reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with Warrington LA.

E-mail

- Pupils only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the learning platform should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The School Website Manager will take overall editorial responsibility and ensure that content is accurate and appropriate. This to be supported by all staff members and issues reported to Headteacher or Website Manager as early as possible.

Publishing pupil's images and work

- Parents and carers sign an agreement so that children's photographs and work can be shared online, (e.g through the website, Class Dojo, Oughtrington School's Twitter account and in online newspaper articles).
- Social networking sites are blocked.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider (EXA) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- See information at the end of this policy relating to filtering.

Managing videoconferencing

- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are switched off during school hours.
- Teachers are encouraged to use the ipads provided to 'Tweet' and use Class Dojo to communicate with parents.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read and adhere to the 'Acceptable ICT Use Agreement' before using any school ICT resource.

Assessing risks

- 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 WBC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Handling Online Safety complaints

- Complaints of Internet misuse by any member of the school community will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a safe guarding nature must be dealt with in accordance with school safe guarding procedures.
- Potentially illegal issues will be referred to the Headteacher

Communications Policy

Introducing the Online Safety policy to pupils

- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic is monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parent/carers' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website.

Appendix 1: Internet use – Possible teaching and learning activities

Activities	Key Online Safety issues	Relevant websites
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	- Google Safe Search
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information.	E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Once Upon a Dream – Young Writer's Competition
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. File names should not refer to the pupil by their full name.	Making the News Museum sites, etc. Digital Storytelling BBC – Primary Art
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype Facetime National History Museum Imperial War Museum

Appendix 2: Procedures to be followed:

1. In the event of pupils being exposed to undesirable materials.

[please see Appendix 3 Definitions]
• The pupils should know to notify a teacher immediately; Online Safety rules are displayed in all classrooms with computer and internet access
• The Headteacher will be notified by the teacher as soon as reasonably practicable
• The incident will be recorded in a central log [overseen by the ICT and Online Safety coordinator] by which the school may reliably report the frequency and nature of incidents to any appropriate body if necessary
• The Headteacher will contact the ISP if appropriate and there are concerns re safe use of the internet
• Parents/ carers and Governors will be notified at the discretion of the Headteacher according to the degree of seriousness of the incident [For example, exposure to materials that include common profanities might not be notified to parents but exposure to materials that included pornographic images would.]

2. In the event of pupils intentionally accessing undesirable materials.

• All pupils will be made well aware of the seriousness of intentionally accessing undesirable materials on the internet and viewing in school. Any incident will be treated as a disciplinary matter and the parents of the child or children will be contacted immediately by the Headteacher. As highlighted above it will be recorded and further advice sought by the school as necessary.
• If deliberate access to undesirable materials is found to be repeated by a pupil or pupils then the matter will be treated very seriously and advice will be sought from the LA or Social Care Team if necessary. The pupil's parents will again be informed and the Governors may be notified regard actions to be taken.

3. In the event of adults intentionally accessing unacceptable materials.

• Deliberate access by any adult to unacceptable material may be treated as a disciplinary matter. The Headteacher must be informed and will act accordingly. Governors may be made aware immediately and the LA will be consulted.

Appendix 3: Definitions

• Undesirable materials

- Pornographic images or obscene text on internet websites or mobile phones
- Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive on websites, text messaging or emails
- Racist, exploitive or illegal materials or messages on websites, mobile phones or emails

• **Undesirable contacts**

- Email messages or text messages from unknown or unverified parties who seek to establish a pupil's identity and/ or communicate with them

• **Unacceptable use**

- Deliberate searching for, and accessing, of undesirable materials
- Creating and transmitting email messages or text messages that contain unacceptable language or content

• **Adults**

- All staff that work in school
- Visitors and guests
- Governors
- Parents/Carers
- Volunteers in school
- Students on work experience placements

Appendix 4: Internet facilities in school

General points

- There are 20 mobile netbooks which are timetabled using google calendar. They are wireless and connected to the internet.
- There are 30 mobile laptops which are timetabled to classrooms for curriculum use. They are all wireless and connected to the internet and the school's network.
- There are 2 banks of 15 Macbooks which are also wireless and mobile
- There are 15 ipads (One per class) linked to the internet and printers
- All classrooms have an internet point so each classroom can have access to the internet through one computer at all times. Teachers based in these rooms have responsibility for ensuring appropriate usage of these connections at all times.
- Teachers using the computers with the children have responsibility for ensuring appropriate usage of these connections at all times.
- All staff can use the classroom computers outside school hours to support them in their work.
- The mobile computers should be kept as a set and not split up.
- There are 4 hard wired computers in EYFS.
- There are 3 hard wired computers in Y1

However, before using the facility it is vitally important that:

- All staff have read the Online Safety policy and the guidelines laid down within it and have signed the Code of Conduct
- All pupils are aware of the Online Safety rules.
- All users have the necessary skills to use the facility safely and for the intended purpose.

Appendix 5 - Standard letter to be sent to parents /carers

Dear Parent/Carers,

As you are aware, all pupils have the opportunity to use the school's computer facilities, including Internet access to aid their learning, as required by the National Curriculum. These facilities are used to enrich and enhance the curriculum. However, it is very important that they are used appropriately and in order to ensure this the school has a detailed online safety policy and online safety rules for all users. We would really appreciate your support in ensuring that the policy is effectively implemented. If you would like to view the policy it is available on the school website or a hard copy can be obtained on request from the school office.

In addition, we would like to ask you to read the enclosed Online Safety Rules that the school has drawn up to ensure appropriate usage of the facilities in school and would ask you to sign to show that you and your child agree with the rules.

If you have any queries about this please contact the school office

Yours sincerely

G Marsland
Head teacher

Appendix 6
Staff (and Volunteer) Acceptable Use Policy Agreement - 2017

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, ipads etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. See Staff Handbook.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person (Eluned Olver, or in cases of safeguarding Gill Marsland).

I will be professional in my communications and actions when using Oughtrington's ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so
- I will only use social networking sites in school in accordance with the school's policies. See Staff Handbook.

- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school / academy*:

- When I use my personal mobile devices (laptops / tablets / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings. If this is required I will request assistance from the technician who will advise.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school / academy*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Appendix 7

Pupil Acceptable Use Policy Agreement KS1 -2017

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

Appendix 8

Acceptable Use Policy Agreement KS2 - 2017

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will not communicate with anyone I do not know.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- The use of personal devices in school is not permitted.
- I will not try to access material which is not appropriate to school.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks unless I know they are trustworthy.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I understand that the use social media is not permitted in school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school* has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may loss of access to the school network / internet, contact with parents and in the event of illegal activities involvement of the police.

I have read and understand the above and agree to follow these guidelines

Name of Student / Pupil: .....

Signed: .....

Date: .....

Parent / Carer Countersignature .....

Appendix 9

Key Stage 2

Online Safety Rules for Key Stage 2

In school we refer to the Online Safety rules as SMART rules.

More detail can be found in Appendix 11

Appendix 11
Parent/Carer's Consent Form

Online Safety Rules – January 2017

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/ carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son / daughter may be published electronically (Class Dojo/ Twitter/ School Website etc) to support learning activities or in materials that promote the work of the school.

Name of Child: ***Signed:***	***Class:*** ***Date:***

Parent's Consent for Internet Access

I have read and understood the school Online Safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
I understand that the school cannot be held responsible for the 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.

Name of Child: ***Signed:***	***Class:*** ***Date:***

Please print name:

Please complete, sign and return to the school office

Appendix 9 –more detail - Smart Thinking

S = Secret

This is about personal information and whether it is safe to give it out. For example, it might apply to an on-line registration form or someone requesting contact details so they can send you a prize.

STOP and **THINK**

WHO wants the information?
WHY are they asking for it?
WHAT will they do with it?

M = Meeting

This is about someone you have never met before contacting you on-line or through a messaging service to invite you to a meeting.

STOP and **THINK**

WHY should you **never** arrange to meet anyone you have only met on-line?
WHAT might happen?
WHO should you tell?

A = Attachments

This is about e-mail and attachments and what you need to think about before opening them.

STOP and **THINK**

WHO sent it?
WILL it be safe to open it?
WHAT can I do to protect myself and the computer?

R = Reliable

Anyone can put anything on the Internet and anyone can use the communication technologies (such as chat, SMS, e-mail, IM) to contact others.

STOP and **THINK**

WHETHER I can rely on information on web sites to be true
WHETHER I can rely on someone I can't see telling me the truth
WHAT can I do to check?

T = Tell

No matter how careful we are, sometimes we might come across things that upset us.

STOP and **THINK**

WHAT can I do when web sites and messages make me feel uncomfortable?
WHO can I tell?
WHAT can I do to stop it happening again?

STOP! THINK! … GO?

Click Aware

We use the Internet with adult permission.

We immediately tell a trusted adult if we see anything that makes us uncomfortable.

We are always polite and friendly when we talk to friends on the Internet (chat, messaging or email).

We always make sure a trusted adult knows about the people we talk to on the Internet.

We never arrange to actually meet people or 'friends' we don't know.

We keep information about ourselves safe and don't share it on the Internet.

We check information we find on the Internet is reliable.

SW GRID for LEARNING

THINK U KNOW

Childnet International

SOMERSET County Council

Developed by South West Grid for Learning Trust and Somerset County Council