Merley First School
Online Safety Policy

Writing and reviewing the Online Safety Policy

- The school is committed safeguarding its pupils and as such, this policy should be read in conjunction with other relevant policies including our safeguarding policies; Behaviour, Code of Conduct and Child Protection policies.
- Our Online Safety Policy has been written by the school, building on the SWGFL Online Safety Policy and government guidance.
- The school's Computing Leader will also act as Online Safety Coordinator.
- It has been agreed by senior management and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Online Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. These are an essential element in 21st century life for education, business and social interaction. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school has a duty to provide children 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 includes 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 educated in 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

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

Information system security

School ICT systems capacity and security will be reviewed regularly.
Virus protection is updated regularly.

E-mail

Pupils may only use approved e-mail accounts on the school system and email usage will be supervised and monitored by a staff member.
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 web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Social networking and personal publishing

The school will block/filter access to social networking sites.
Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location.
Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

The school will work with the LA, SWGFL and the Internet Service Provider 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.

Managing video conferencing

Pupils will be required to gain permission from the supervising teacher before making or answering a video conference call.
Video conferencing will be appropriately supervised for the pupils' age.

Managing emerging 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 will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

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

Authorising Internet access

All staff must read and sign the 'Staff (and Volunteer) Acceptable Use Policy Agreement' before using any school ICT resource.

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or a pupil's access be withdrawn.

For Key Stage 1, access to the Internet will mainly be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form when the child (children) start in reception.

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 or iPad.

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 will be dealt with by the head, deputy or assistant head.

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Introducing the Online Safety policy to pupils

Online Safety rules and safety guidance will be posted in the Computing Suite and discussed at certain points throughout the 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 can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Education – parents / carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents evenings and information sessions
- High profile events / campaigns e.g. Internet Safety Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk http://www.childnet.com/parents-and-carers

Use of digital and video images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (may be covered as part of the Acceptable User Policy signed by parents or carers at the start of the year).
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Staff/volunteers private use of digital media

In their private use of digital media (such as social networking sites) staff must protect their professional reputation and that of other Trust staff and staff in partner organisations. This must be achieved either through the judicious application of privacy settings so that communications remain private from children and young people / parents and carers and through the avoidance of rhetoric that might cause reputational damage.

Staff/volunteers must not solicit or accept "friend / contact / circle / follow" type connections to private accounts with children and young people for whom they have any professional responsibility.

Staff/volunteers must not engage in any communication which could bring the Trust/school into disrepute which includes postings made on personal sites, blogs in staff's own time. Staff must be mindful of confidentiality and data protection. If a staff member becomes aware that they have posted a comment which may bring the Trust into disrepute or breach data protection they must bring this to the attention of their manager urgently, who in turn will seek advice from the Headteacher and Executive Headteacher (where appropriate). The Trust's HR provider may get involved after that if the manager needs help to deal with the individual's behaviour and its impact via the Disciplinary Procedures.

At all times staff must be respectful of others, not engaging in any communication which could be deemed as breaking the law regarding discrimination or offensive behaviour. They must never use social media to bully or harass another employee, manager or service user including any child or young person.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *Online Safety / Computing* Governor. The role of the Online Safety / Computing Governor will include:

- regular meetings with the Online Safety / Computing Co-ordinator;
- regular monitoring of Online Safety incident logs;
- regular monitoring of filtering / change control logs;
- reporting to relevant Governors at a committee meeting.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		yes						yes
Use of mobile phones in lessons				yes				yes
Use of mobile phones in social time	yes							yes
Taking photos on school camera	yes				yes			
Use of hand held devices eg PDAs, PSPs		yes						yes
Use of personal email addresses in school		yes						yes
Use of school email for personal emails				yes				yes
Use of chat rooms / facilities				yes				yes
Use of instant messaging				yes				yes
Use of social networking sites				yes				yes

When using communication technologies the school considers the following as good practice:

- The official *school / academy* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the school / academy email service to communicate with others when in school, or on school / academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school / academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1 and KS2.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Enforcement

Breaches of this policy will fall into the following categories:

- Illegal acts by staff – Escalated to Police/LADOs/Children's Social Care;

- Breaches of policy – Following investigation by LADOs / Children's Social Care/HR/Data protection as appropriate, these are handled by line managers in accordance with the standard disciplinary procedures.

Supporting information

http://ceop.police.uk - For advice and guidance from the Police's Child Exploitation and Online Protection Unit (CEOP);
http://www.swgfl.org.uk - Staying-Safe For Online Safety support material from the South West Grid for Learning who provide Internet connectivity to nearly all state schools in the 15 South West local authorities as well as actively managed filtering and monitoring. This includes Standard Acceptable User Policies, bring your own device, advice on clouding etc.
http://www.iwf.org.uk - Internet Watch Foundation ,for the reporting of criminal online content;
http://webarchive.nationalarchives.gov.uk/20100202101002/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311 - Guidance for safer working practice for adults who work with children and young people – government 2009;
http://www.e2bn.org/files/Inspecting_Online Safety.pdf -Inspecting Online Safety Ofsted 2012;
https://www.gov.uk/data-protection the-data-protection-act Data Protection Act 1998;
http://webarchive.nationalarchives.gov.uk/20130401151715/
https://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf
Byron review 'Safer children in a digital world';
http://webarchive.nationalarchives.gov.uk/20120408131156/http:/www.ofsted.gov.uk/resources/safe-use-of-new-technologies Safe use of new technologies Ofsted 2009;
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis UK Council for Child Internet Safety;
http://www.nspcc.org.uk/Inform/research/briefings/Photographing-children_wda96007.html NSPCC guidance on photos in schools;
https://ico.org.uk/for-organisations/guide-to-data-protection/
Safe Schools and Communities team ssct@dorset.pnn.police.uk 01202 222844. This team provides support if an E safety incident occurs as well as training packages for children, young people, parents/carers and staff.

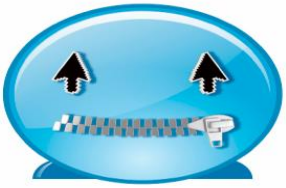
Date of Policy	Minute No	Date due for review
March 2016	To be approved by FGB	March 2017

Appendix 1

Online Safety Safety Rules Foundation, YR 1 and 2

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Children/young people and adults in the school are learning how the values and principles of the UNCRC help to create a safe and secure environment. Parents and carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Think then Click		
These rules help us to stay safe on the Internet		
	We only use the internet when an adult is with us	
	We can click on the buttons or links when we know what they do.	
	We can search the Internet with an adult.	
	We always ask if we get lost on the Internet.	
	We can send and open emails together.	
	We can write polite and friendly emails to people that we know.	



ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

Article 13: Children have the right to get and share information, as long as the information is not damaging to themselves or others.

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.

Child's name:……Class:……Date:……

Signed:……Name (please print)……

Appendix 2

Online Safety Safety Rules YR 3 and 4 (Lower Key Stage 2)

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Children/young people and adults in the school are learning how the values and principles of the UNCRC help to create a safe and secure environment. Parents and carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

Article 13: Children have the right to get and share information, as long as the information is not damaging to themselves or others.

Pupil's Agreement

- I have read and I understand the school Online Safety Rules;
- I will use the computer network, Internet access and other new technologies in a responsible way at all times;
- I know that network and Internet access may be monitored.

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.

Child's name:……Class:……Date:……

Signed:……Name (please print)……

Appendix 3

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school may monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school.

- I understand that the school ICT 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.
- 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 will immediately report any illegal, inappropriate or harmful material or incident when I become aware of it to the appropriate person.
- I will be professional in my communications and actions when using school 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. Where these images are published (e.g. on the school website / Virtual Learning Environments) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with 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, the Wimborne Academy Trust and LA have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / 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 also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses in school on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- 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, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / Trust / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- 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 school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school 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, Trust 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 ICT 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:……