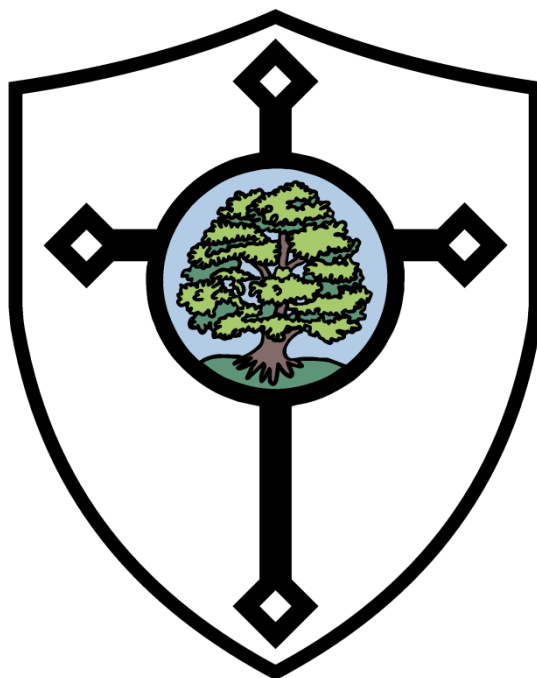


The New Forest C of E (VA) Primary School
at Landford, Nomansland & Hamptworth



**E-safety
and Acceptable Use of IT
Policy**

Adopted: March 2015

Last reviewed/approved: December 2018

Review: two yearly

Status: non-statutory

E-safety and Acceptable Use of IT Policy

The New Forest Church of England Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff, governors and volunteers to share this commitment. We have adopted the *'Fruits of the Spirit'* (Galatians 5:22) as our school values and expect these to be demonstrated by everyone in our school in accordance with our mission statement *'Growing and Learning Together through Christian Values'*.

1. Rationale

Schools have the opportunity to transform and enhance education and help children to fulfil their potential and raise standards with ICT. However, schools also have a duty of care and must ensure that they are able to safeguard children and staff, so it is also important that children learn how to be safe when they are using new technologies.

At The New Forest Primary School, whilst blocking and banning is part of our policy, we believe a more sustainable approach is required. We will equip the children with the skills and knowledge they need to use the Internet safely and responsibly, managing the risks wherever and whenever they go online; to promote safe and responsible behaviours in using technology both at school and in the home and beyond. What are the risks? The Byron Review (Safer Children in a Digital World 2008) classified the risks as relating to content, contact and conduct. The risk is often determined by behaviours rather than the technology itself.

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading information/ advice
Contact (Child as participant)	Tracking Harvesting personal information	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing one another	Creating and uploading inappropriate material	Providing misleading information/advice

2. Internet access

The Internet is an essential element in 21st century life for education, business, and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Internet use will enhance learning opportunities and is part of the statutory curriculum and a necessary tool for staff and pupils.

The school will:

- Ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Ensure that our 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.
- Educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Shown how to publish and present information to a wider audience.
- Taught how to evaluate Internet content.
- Taught the importance of cross-checking information before accepting its accuracy.
- Taught how to report unpleasant Internet content.

3. E-mail

- There are no pupil email accounts currently available to children.
- Pupils may only use approved e-mail accounts on the school system e.g. when sending work from the IPAD to be printed.
- Pupils are taught about how to communicate using email outside of school as part of the PSHE and Computing schemes of work, e.g. not sharing personal data with unknown people.
- All staff are issued with a school email account that they are expected to use for school use. Please also refer to the school's Data Protection Policy.

4. Published content and the school website

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Where possible group photographs will be used rather than full face photos of individual children.
- Pupils' names will not be used in association with photographs anywhere on the school website or other on-line space.
- Pictures and work will only be shown on the website if parents/carers have signed the consent form issued at the start of each school year.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. Please also refer to the school's Data Protection Policy.

5. Social networking, curriculum games and personal publishing

- If they are to be used, the school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils would use only moderated social networking sites appropriate to age.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

6. Managing videoconferencing and webcam use

When available, videoconferencing and webcam use will be appropriately supervised for the pupils' age.

7. 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.
- Staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Games machines, including the Sony Playstation, Microsoft Xbox and others, have Internet access which may not include filtering. These may not be used in school.

8. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Please refer to the school's Data Protection Policy.

9. Procedures

- The School ICT system's security will be reviewed regularly.
- Virus protection will be updated regularly.
- Acceptable use posters will be displayed in each classroom and on the laptop charging trolley.
- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider (South West Grid for Learning) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Senior Leadership Team and the school Network Manager and the E-Safety Coordinator informed.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school will use the RM Securenet Plus filtering service through the 'South West Grid for Learning' (SWGfL) to ensure adequate filtering is in place. The filtering settings may be adjusted by authorised personnel (teachers) to enable access to certain web content that might automatically be restricted such as YouTube. Any settings that are adjusted must be temporary and the filters should be made secure once again after the specific web content has been viewed. All filtering passwords will be kept securely and will only be issued by the Head Teacher.
- The school should audit ICT use to establish if the safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.
- E-Safety training will be embedded within the Computing scheme of work and alongside the Personal Social and Health Education (PSHE) curriculum.
- E-Safety briefings and materials will regularly be made available to parents.
- Staff will always use a suitable and safe search engine when accessing the web with pupils.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone.
- Should special circumstances arise where such communication is felt to be necessary, the agreement of Senior Leadership should be sought first and appropriate professional language should always be used.

- Staff must not use mobile phones during teaching time or use camera phones except for the need to access CPOMS authentication codes.

10. Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the Head Teacher.
- 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 the school's child protection procedures and be directed to the designated person for child protection.
- Pupils and parents will be informed of the complaints procedure (see schools Complaints Procedure).
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

11. Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school website.
- The school will ask all parents to sign the parent/pupil agreement at the start of each school year or when children are admitted in the case of in-year admissions.

12. Rules for acceptable internet use

The school has installed computing equipment and Internet access to help our learning.

The school has agreed internet and computing equipment rules to keep everyone safe and help us be fair to others.

Posters are displayed prominently and we provide pupils and parents with copies of these rules (see Appendix A).

13. Staff rules for acceptable use of ICT

The school has installed computers and Internet access to help us fulfill our role within the school.

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

- The Head Teacher is the designated E-safety Coordinator along with Designated Safeguarding Lead.
- All staff should use school based email accounts (not hotmail or others) for school related emailing. (a.name@thenewforestschoo.wilts.sch.uk)
- Staff do not respond to emails from school pupils except on the school email account.
- Social networking sites are not accessible via the school network due to filtering by SWGfL.
- Staff must not become 'friends' with pupils on social networking sites (unless direct family members).
- The school strongly recommends that staff members are not 'friends' with parents from school on social networking sites.
- Do not give out your personal mobile phone number to students or parents.
- Turn Bluetooth off your phone whilst in school.
- Do not use personal mobile phones for school business except for CPOMS authentication codes. The school has a 'pay as you go' mobile phone for use during trips and other emergency situations.
- Only use school cameras and computers to take and store photos of pupils.
- Do not use your mobile phone to take photographs or videos of pupils and school activities
- Report all inappropriate images/sites that have been found to be unacceptable on the school network to the Senior Leadership team and E-safety coordinator.
- Refer to the school's whistle blowing procedures if you believe any staff member is not following these rules.
- Any adjustments to the filtering service must be authorised and temporary.

Staff members are asked to sign an agreement (see Appendix B) to ensure that everyone has fully understood the requirements for protecting both children and staff when using ICT.

14. Writing and reviewing the E-safety policy

The school's E-Safety Coordinator is the Designated Safeguarding Lead as the roles overlap.

Our E-Safety Policy has been written by the school. It has been agreed by all staff and approved by the Governing Board. The implementation of this policy will be monitored by the Computing subject leader and Head Teacher who will in turn report to the Governing Board's Resources Committee.

Related policies:

- Anti-bullying Policy
- Behaviour Management Policy
- Computing Policy
- Data Protection Policy
- Personal Social and Health Education (PSHE) and Citizenship Policy
- Safeguarding and Child Protection Policy
- Whistleblowing Policy

Useful websites:

www.becta.org.uk

www.teachernet.gov.uk

www.thinkuknow.co.uk/teachers

www.childnet.com

www.kidsmart.org.uk

www.ceop.gov.uk/reportabuse/index.asp

www.everychildmatters.gov.uk

Appendix A: Internet safety posters

Internet Safety Poster used at Key Stage 1 Landford



The New Forest Church of England (VA) Primary School
at Landford, Nomansland and Hamptworth


Computer & Internet
Think then Click!



These rules help us to stay safe on the computers and internet:


- We only use the computers with permission.
- We always ask before printing anything.
- 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 e-mails together.
- We can write polite and friendly e-mails to people that we know.

Internet Safety Poster used at Key Stage 2 Nomansland



The New Forest Church of England (VA) Primary School
at Landford, Nomansland and Hamptworth

Computer & Internet Safety
Think then Click!



These rules help us to stay safe on the computers and internet:

- We only use the computers with permission.
- We always ask before printing anything.
- We ask permission before using the internet.
- We only use websites that an adult has chosen.
- We only search the internet with an adult's supervision.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are 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.

Appendix B



**The New Forest Church of England (VA) Primary School
at Landford, Nomansland and Hamptworth**

Code of Conduct for ICT - Staff Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's E-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Head Teacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission of the ICT Leader or Head Teacher.
- I will not use my mobile phone to take photographs or videos of pupils or school activities.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises, or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Leader (Head Teacher).
- I will ensure that electronic communications with pupils including email and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood, and accept the Staff Code of Conduct for ICT:

Signed: Print name: Date:

Accepted for school: Print name: