Maendy Primary School

E-Safety And Acceptable User Policy

Date of this review: Autumn 2016
Date of next review: Autumn 2017

Signed: …….. **Date:** ……

Chair of Governors

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications as well as 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 school's e-Safety policy operates in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

This core e-Safety policy provides the essential minimal school e-Safety policy.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-Safety policy in both administration and curriculum, including secure school network design and use.

E-Safety Audit

This quick self-audit will help the senior leadership team (SLT) assess whether the e-Safety basics are in place to support a range of activities.

Does the school have an e-Safety Policy?	√
Date of first e-Safety policy: 18th November 2008	
The policy was agreed by governors in: November 2015	
The policy is available for staff at: School Intranet (U Drive) and website.	
And for parents/wider community at: School Web site -http://www.maendyprimary.co.uk	
The designated Child Protection Officer is: Mrs J Cresswell	
The designated e-Safety Coordinator is: Mrs J Cresswell	
Is e-safety training provided for pupils, staff and governors?	√
Do all staff sign an ICT Code of Conduct on appointment?	√
Have school e-Safety Rules been set for pupils?	√
Do pupils sign an agreement that they will comply with the School e-Safety Rules?	√
Internet access is provided by an approved educational Internet service provider	√

and complies with DfES requirements for safe and secure access.	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	√

School E-Safety policy

The points below are the essential minimum points for our school e-Safety Policy. The aim of this policy is to protect pupils and educate them to be responsible when using ICT.

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- The school has an appointed e-Safety co-ordinator: Mrs J. Cresswell
- The school's e-Safety co-ordinator is responsible for the leadership of the e-Safety group (established Autumn 2015, which includes members of senior management/staff governors).
- The roles of the designated Child Protection co-ordinator will sometimes overlap.
- Our e-Safety Policy has been written by the school. It has been agreed by the school's e-safety group and is approved annually by governors. Updates to the policy may be informed by pupil and parental feedback.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was created by: Miss J Clancy in September 2008
- It is approved annually by the Governors during the Autumn Term.
- The nominated e-Safety Governor is: Mr. Andrew Prothero-Jones.

Teaching and learning

Why Internet use is important?

- 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 is a part of the statutory curriculum for ICT and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school's E-safety scheme of work sits within the ICT and PSE curriculums. The school uses CEOP ThinkuKnow materials together with the SWGfL Digital Literacy & Citizenship materials in a progressive program which ranges from Reception to year 6.
- The school Internet access is designed expressly for pupil use.
- Pupils are taught what type of Internet use is acceptable and what is not. They are given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation (Information Literacy).

Pupils will be taught how to evaluate Internet content

- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught (where appropriate) to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- The school ICT systems, capacity, security, filtering and virus protection is the responsibility of the LEA.

Password Policy

- All staff have secure passwords that comply with LEA guidelines. These are changed on a regular basis and may be changed upon request. Administrator passwords are used only by the ICT co-ordinator, when deemed necessary by the LEA technical support team. Pupils are provided with secure, age-appropriate passwords for Purplemash, Giglets and Hwb+ and are encouraged not to share their login details with any other pupils.

E-mail

- Pupils may only use approved Microsoft Outlook class e-mail accounts on the school network.
- 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 before sending, in the same way as a letter written on school headed paper.

Published content and the school web site / Twitter feed

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

Cloud-based Storage

- Work created using iPads is stored securely online using the cloud storage space, Microsoft OneDrive. Pupils who do not have written permission for digital imagery consent (see below) will not be permitted to upload content containing images of themselves.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will comply with digital imagery consent. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site, Twitter feed or YouTube channel.

- A Digital Imagery consent record is kept (and continually updated) to show those pupils who do/do not have digital imagery permission. The spreadsheet is broken down into a "blacklist" to clearly identify pupils in each year group for whom parental permission has not been obtained.
- Pupil's work can only be published with the permission of the pupil and parents.
- Pupils' full names will not be used on the website or Twitter feed.

Social networking and personal publishing

- The school blocks/filters access to social networking sites.
- Newsgroups are blocked unless a specific use is approved.
- Pupils are taught never to give out personal details of any kind which 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.
- Video Conferencing projects are organised by teaching staff and pupils are supervised at all times during the session. Permission from parents is sought before any pupil becomes involved in video conferencing projects at a local, national and international level. Any work that is produced by pupils and requires an exchange with another organisation will not be dispatched unless permission is granted by parents or guardians.
- Hwb+ is used as a safe, secure, online virtual learning environment (VLE) accessible to all staff and pupils, advocated by the Welsh Government as an all-Wales learning platform. Pupils are made aware that the content which they publish on the learning platform is made public for all members of the school community to see and is monitored by staff.

Managing filtering

- The school works with the LEA to ensure systems to protect pupils are reviewed and improved whereby a firewall (such as the Barracuda web filter) will be used to filter out any unsuitable websites.
- Pupils using websites for research will be advised to use recommended child-friendly sites, such as BBC Education, wikipedia, etc.
- Pupils are able to access video sites, such as You Tube. Welsh Assembly Government recommends that schools should not fire wall such sites, but teach pupils how to use the Internet safely. Therefore, they endorse health and safety on the Internet.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety group (See **Reporting an e-safety concern** section below).
- Children will also be taught Health and Safety on the Internet and are advised on how to act if they bring up any search results that make them feel uncomfortable.

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

- CEoP / e-Safety training is delivered annually to make all staff aware of safe and acceptable use of the Internet. All staff are asked to sign and agree to an 'Acceptable use of ICT' policy *[Appendix 1]* annually.
- The school keeps 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.
- At Key Stage 1, access to the Internet is by adult demonstration with occasional directly supervised access to specific, approved on-line materials (e.g. Purplemash).
- At Key Stage 2, access to the Internet is by adult supervision to approved on-line materials.

Assessing risks

- The school takes 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. Maendy Primary cannot accept liability for the material accessed, or any consequences of Internet access.
- The school has been using the '360 degree safe' online self-evaluation tool since January 2015, which is enabling us to evaluate our existing position regarding e-Safety and target improvement.

Policy scope

- Staff personal mobile devices/technology is to be used appropriately in line with the Staff Acceptable Use Policy for ICT, in order to minimise risk of sensitive information becoming inadvertently compromised.
- A form must be completed by parents/carers to give permission for pupils to bring a personal mobile device into school, which must be given to the class teacher. *[Appendix 5]*Pupils are prohibited from using these devices during school time. Any device found without permission will be confiscated and must be collected by the parent/carer of the pupil.
- The school is not liable for any damage or loss.

Reporting an e-safety concern

- At Maendy, we show a commitment to act on e-Safety incidents outside the school, as well as in school, through the use of the 'Report of an E-Safety Concern' proforma, introduced in Autumn 2015 *[Appendix 4]*, which can be used by pupils, staff or parents to raise awareness of an issue that may have occurred in school or at home (which links to school). The proforma should be completed and returned immediately to a member of the e-Safety team.
- These "Report of an e-safety concern" forms have been created by the e-Safety group, with consultation from staff and School Council members.
- Collected forms will be monitored by the e-Safety team and logged in a file, to be kept by the e-Safety co-ordinator.

- Any further action required may then be taken if necessary (i.e. Report filtering issue to SRS team to be dealt with, Child Protection referral etc.) Complaints of a Child Protection nature must be dealt with in accordance with school Child Protection procedures.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Pupils who do not adhere to the e-Safety rules and procedures (outlined in the Pupil Acceptable Use Agreement) will be treated in line with the sanctions identified in the school's behaviour policy.

Communications

Staff and the e-Safety policy

- This policy is developed in consultation with a wide range of staff.
- All staff have access to the School e-Safety Policy and its importance explained.
- Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Introducing the e-Safety policy to pupils & parents

- E-Safety rules and posters are displayed in the ICT suite and discussed with the pupils at the start of each year. Pupils sign an acceptable user agreement *[Appendix 2]* to show that they understand the systems in place. This is acknowledged by parents.
- Pupils and parents are informed that network and Internet use is filtered.
- E-Safety requirements and information (acceptable use agreements and digital consent agreements) are included in the induction process for new pupils and parents.

Enlisting pupils' & parents' support

- Parents' and carers' attention is drawn to the School e-Safety Policy via the School prospectus and also on the School Web site, and planned workshops will also be used from Spring 2015.
- Parent/Carer and pupil surveys will be used (from Autumn 2015) to help identify any weaknesses and/or strengths with regard to our E-Safety practise/policy.
- Parents are asked to sign a Parent/Carer Acceptable use of ICT agreement *[Appendix 3]* to show understanding that making critical, derogatory or malicious comments about the school on social networking sites (i.e. Facebook, Twitter) is unacceptable and may result in legal action.

[Appendix 1]

Maendy Primary School
Staff Acceptable Use Policy for ICT

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; PDAs; digital cameras; e mail and social networking and that only ICT only authority owned (School) equipment should be 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 e mail 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.
- I will not install any software or hardware without permission from the Head Teacher.
- 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 right and adhere to the Data Protection Act 1998.
- I will report any incidents of concern regarding children's safety to the e-Safety co-ordinator, the Designated Child Protection Co-ordinator or Head Teacher.
- I will ensure that electronic communications with pupils including email, instant messaging 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.

Breach of the policy will be considered a serious disciplinary matter and will be dealt with in line with the Disciplinary Policy and procedure.

I have read, understood and accept the Staff Acceptable Use Policy for ICT.

Signed: …… Print Name: …… Date: ……

Accepted for School: …… Print Name: ……..

[Appendix 2]

Student / Pupil Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure that:

- Pupils will be responsible users and stay safe while using school systems and devices.
- School systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at potential risk.

Acceptable Use Agreement

I understand that I must use school systems and devices responsibly, so that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I understand that my use of the Internet in school will be monitored.
- I will not use a personal device that I have brought into school.
- I will not try to access any materials that are inappropriate or may upset others.
- I will immediately report any inappropriate material or incident, I become aware of, to a member of staff.
- I will not access, change or delete any other pupil's files, without permission.
- I will only take images of other pupils with their permission. I will not use any personal equipment to record images.
- I will not publish or share any information about school on any personal website or social networking site, unless I have permission from the school.
- I will not install programmes of any type on a school device, nor will I try to change computer settings, unless I have permission to do so.
- I will not cause any damage to school ICT equipment.
- I will report any damage or faults involving equipment or software, to a member of staff.
- Where work is protected by copyright, I will not download or share copies (including music and videos).

- I understand that if I fail to follow this Acceptable Use Agreement, the school has the right to stop me from using school Internet systems / devices.

I have read and understood 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 about the school) within these guidelines.

Name

Signed

Date

[Appendix 3]

Parent / Carer Acceptable Use of ICT Agreement

The use of social networking sites is not an appropriate media to voice or resolve any concerns you and/or other parents/carers may have about the school.

Our school has an 'open door policy' in relation to any concerns that you and/or other parents/carers may have about the school. The school further implements a complaints procedure which is available to parents/carers on request or through our website.

The school has an e safety policy, which it employs in relation to staff, school pupils as well as parents/carers on social networking and cyber bullying issues. This policy identifies expectations that parents/carers should adhere to. You may view the policy on our website or view the hard copy at the school by appointment. If you have genuine concerns regarding the school then you are asked to make an appointment with the head teacher or Family Liaison Officer.

I understand that, as a parent/carer of a pupil in the school, making critical and/or derogatory or malicious comments about the school on social networking sites (i.e. Facebook, Twitter) is unacceptable and may result in legal action.

Signed _____ Date _____

Child's name/Year group _____

[Appendix 4]

Dear pupils, parents and carers, staff and members of the wider school community,

Report of an E-Safety Concern

(Introduced Autumn 2015 & ratified by School Council)

If you have a concern over any aspect of E-Safety, please complete this form and return it to a member of staff who will pass it on to a member of the school's E-Safety Team.

Name	
Date	
Time	
What is your concern?	
Please give names if you can Where were you when you became concerned worried? Who else was there?	
Who else knows about this?	
If you think that someone may be upset, please can you provide give their name?	
Could anyone be at risk in danger because of this?	

Thank you for completing this form!

Mr Edwards, Mr Morgan, Mrs Rosser, and Mrs Cresswell (The E-Safety Team).

Action taken:	
By Whom:	
Date:	

[Appendix 5]

MAENDY PRIMARY SCHOOL
Wayfield Crescent
Northville
Cwmbran
NP44 1NH

Headteacher: **Mrs J Cresswell**
Telephone : **(01633) 483168**
E Mail: **head.maendyprimary@torfaen.gov.uk**
Web Address: **maendyprimary.co.uk**

Dear Parent/Carer

MOBILE PHONE PERMISSION FORM
Please complete, sign and return this form to Mrs J Cresswell at Maendy Primary School.

I give permission for my son/daughter to bring their mobile phone into school for emergency use. This will be kept safe with the class teacher:

Name of pupil: ……..

Parent Signature …….. Date: ……..

A copy of the e-Safety policy (with a section relating to the use of mobile phones) can be viewed on our website.

Yours sincerely

J CRESSWELL
HEADTEACHER