



Datchet St Mary's C of E Primary Academy

E-Safety Policy

Why does our school need an E-Safety Policy?

- The exchange of ideas, social interaction and learning opportunities provided by electronic communication technologies are greatly beneficial to all, but can occasionally place children, young people and adults in danger.
- E-safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.
- We believe there is a balance to be struck between controlling access to the internet and technology, setting rules and boundaries and educating children and staff about responsible use. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns.
- All members of staff need to be aware of the importance of good e-safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.
- This E-Safety Policy is essential in setting out how the school plans to develop and establish its e-safety approach and to identify core principles which all members of the school community need to be aware of and understand.

The computing co-ordinator is the deputy designated safeguarding lead and the designated safe guarding lead is the Headteacher. There is a governor with a specific responsibility for safeguarding and e-safety. This Policy is part of many different school policies including the ICT, Child Protection, Anti-bullying and PSHE policies. It has been written by the school, building on government guidance.

The E-Safety Policy and its implementation will be reviewed annually.

1.2.1 Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide children with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

1.2.2 How does Internet use benefit education?

Benefits of using the Internet in education can include:

- Raised standards of attainment for children
- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational
- Materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and
- Automatic system updates;
- Exchange of curriculum and administration data with the DfE;
- Access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Children will learn digital literacy skills which are so important in the 21st Century.
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research.

1.2.4 How will pupils learn how to evaluate Internet content?

- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

1.3 Managing Information Systems

1.3.1 How will information systems security be maintained?

The school will seek advice from RBWM and ODST regarding SIMS security

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Devices should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan. This includes memory sticks. Portable media to be checked for viruses using anti-virus scanning application before use.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced and will be changed at least 3 times per year.

1.3.2 How will email be managed?

Email is central to effective communication throughout the school and all staff are encouraged to access their individual email accounts regularly. All school staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business.

- Pupils may only use approved email accounts for school purposes and under the direct supervision of a teacher.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole -class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- To send emails to external organisations the school has access to First Class through the school office which is a secure email system. The school are also able to password protect any sensitive documents using the office 365 email system.
- Staff should not use personal email accounts during school hours or for professional purposes.

1.3.3 How will published content be managed?

Publication of any information online should always be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Senior Leadership team will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

1.3.4 Can pupils' images or work be published?

At Datchet St Mary's Primary Academy the security of staff and children is paramount and the online publishing of children's names with their images is not acceptable. Images of pupils will not be published without the parent's or carer's written permission.

Pupils also need to be taught the reasons for caution in publishing personal information and images online (see section 2.3.6).

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will be used on the website, with signed parental permission
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The school has a policy regarding the use of photographic images of children which outlines policies and procedures.

1.3.5 How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

1.3.6 How will filtering be managed?

Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access

and that Acceptable Use Policies are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online. There should also be an Incident Log to report breaches of filtering or inappropriate content being accessed. Incidents should be reported to the Headteacher who will report such incidents to parents and RBWM or the e-Safety Officer where appropriate.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF, Thames Valley Police or CEOP (see e-Safety contacts and references).

Websites which schools believe should be blocked centrally should be reported to the Computing Coordinator. Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with RM Education to ensure that filtering policy is continually reviewed.
- The school run a weekly check on the RM filters program that is reported to the Head Teacher
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Thames Valley Police or CEOP
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

1.3.7 How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

1.3.8 How should personal data be protected?

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

1.4 Policy Decisions

1.4.1 How will Internet access be authorised?

- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.

1.4.2 How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

1.4.3 How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in RBWM.

1.4.4 How will e–Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e-Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

1.4.5 How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on antibullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- The Police will be contacted if a criminal offence is suspected.

1.4.6 How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use Policy
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in classrooms or the

Staff Room.

1.4.6 Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will use the school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

1.5 Communication Policy

1.5.1 How will the policy be introduced to pupils?

Children will be explicitly taught about e–Safety. This could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever pupils are using the internet.

Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Orange Education: www.orange.co.uk/education
- Safe: www.safesocialnetworking.org
- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.

1.5.2 How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

1.5.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e-Safety at other attended events e.g. parent evenings.

Policy produced by.....**ICT Subject Leader**.....

Signed..... Print.....

Date.....

Review Date.....**October 2018**.....