Crockerton Church of England Primary School

Potters Hill, Crockerton, Warminster, Wiltshire, BA12 8AB
Web: www.crockerton.wilts.sch.uk Tel: 01985 212168
Headteacher: Mrs Nic Ilic

VISION STATEMENT
Together we learn and grow, beyond expectations, guided by our faith and values.

Be joyful. Grow to maturity. Encourage each other. Live in peace and harmony.

2 Corinthians 13:11

Online Safety Policy

This is a single policy which has been written on behalf of the Governing Body for Crockerton Church of England VA Primary School.

Written	**December 2016**
Reviewed	**December 2022**
Author	**Computing Subject Leader & Head Teacher**
Next Review	**December 2023**

We are committed to safeguarding and promoting the welfare

of children and young people

Crockerton Primary School believes in the educational benefits of Digital Technology for effective teaching and learning practices. Secure and effective internet access for pupils is seen as an entitlement on the basis of educational need and an essential resource for staff. As a school we recognise online safety issues and plan accordingly to ensure appropriate, effective and safe use by all.

The Policy

This document has been written with the following key principles in mind:

- All users are protected from inappropriate material, bullying and harassment.
- Users have access to resources to support learning and teaching.
- Users should be given clear boundaries on responsible and professional use.

This policy should be read alongside the Safeguarding and Child Protection policy, Staff Behaviour policy, Responsible User policy, Behaviour policy, Anti-bullying policy, Home-School agreement, Computing policy.

1. Leadership and Management

1.1 Developing a policy

Our online policy has been written by the school, building on the Wiltshire online template policy and government guidance. It has been agreed by senior teachers and approved by governors. It will be reviewed annually.

1.2 Authorised Access

- The school receives Internet Service Provision (ISP) from Soft Egg and will request monitoring reports from the ISP, which will be regularly checked to identify any attempts be to access illegal content and would notify the local police and Wiltshire Council in these instances.
- 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 The record will be kept up to date; for instance if a pupil's access is withdrawn.
- Primary pupils' home-school agreement will include the Responsible Use Policy (Appendix 2) and guidance for sound, image and video for publication online.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible. At Key Stage 2, pupils will able to search the internet independently, but will be supervised at all times.
- Parents will be informed that pupils will be provided with supervised Internet access.

1.3 Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

- A designated member of staff will review the popular permitted and banned sites accessed by the school.

- The school will work in partnership with parents, Wiltshire Council, Dept. For Education (DFE) and its ISP to ensure systems to protect pupils are reviewed and improved regularly.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the Head Teacher.
- Website logs will be regularly sampled and monitored by the Computing Subject Leader and reported to head teacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities.

1.4 Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue but it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

2. Teaching and Learning

2.1 The Curriculum

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. There is no statutory requirement in the EYFS curriculum but best practice supports that pupils in the EYFS gain an understanding of online safety, and this is built into the Computing Curriculum.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.
- The Internet is an essential part of everyday 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.
- 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 school has an Online Safety Curriculum that is taught at the beginning of each academic year, revisiting and building upon prior learning. The learning is in depth with the aim of setting clear expectations, guidance and skills for safe internet use for all pupils.
- Other areas of the Computing Curriculum allow for regular revisiting of online safety skills throughout the year.
- Throughout the year, the school work with local PCSOs, the NSPCC and other agencies to deliver assemblies and Online Safety Days.

2.2 Enhancing Teaching and Learning

Benefits of using the Internet in education include:

- Access to a variety of worldwide educational resources
- 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
- Access to learning wherever and whenever convenient.

2.3 Evaluating Content

- Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- 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.
- If staff or pupils discover unsuitable sites or content, they consider to be inappropriate, the URL (address) and content should be reported to the Computing Subject Leader or ISP/SWGfL
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

3. Communication and Content

3.1 Website Content

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

- The point of contact on the school website should be the school address, school email and telephone number. Staff or pupils' personal information will not be published.

- Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the school website. (Appendix 1 - General Consent form and letter).
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The nature of all items uploaded will not include content that allows the pupils to be identified.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.2 Managing email

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects between schools. However, the use of email requires appropriate safety measures.

- Pupils may only use approved email accounts on the school system and should be used in an acceptable way.
- Sending images without consent, explicit images, messages that cause distress and harassment to others or are considered significant breaches of school rules and will be dealt with accordingly.
- Pupils must immediately tell a responsible adult if they receive offensive or distressing email.
- Staff and governors must use secure email for all professional communications and wherever possible, this should be via an official school provided email account
- Email sent to an external organisation should be written carefully and, where appropriate, authorised by Head Teacher or Admin. Officer before sending, in the same way as a letter written on school headed paper.
- Pupils must not reveal details of themselves or others in email communication, or arrange to meet anyone.

3.4 On-line communications and Social Media

On-line communications, social networking and social media services may be filtered in school by their ISP but are likely to be accessible from home.

- Users will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Users must not reveal personal details of themselves or others in online communication or to arrange to meet anyone.
- Staff wishing to use Social Media tools with pupils 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 consent from the Head Teacher before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and only operate with approval from the Head Teacher.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
- Parents wishing to photograph or video at an event should be made aware of the school's expectations that such pictures including children other than their own, are for home use only and not to be put on social media platforms.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites.
- 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 Responsible Use Policy (Appendix 3).
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people. Where there is communication between parents and/or carers, personal references to the school and any pupils or staff must be avoided. Express care is also to be taken regarding the use of social networking sites.

3.5 Mobile Devices (Including Bring Your Own Device-BYOD) (see Mobile Phone Policy)
Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

Pupil mobile phones are not permitted within the school except in exceptional circumstances and with the Head Teacher's permission. They must be handed to the Office. Unless agreed otherwise.

- Sending abusive or inappropriate messages or content is forbidden by any user within the school community and would be taken very seriously
- Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. email, phone, class dojo) In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to the Head Teacher ASAP.
- Staff should be provided with school equipment for taking photos or videos of pupils linked to an educational intention. In exceptional circumstances staff may need to use personal devices for such a purpose and when doing so, should ensure they comply with the school's Responsible Use Policy (Appendix 3) and notify the Head Teacher ASAP.
- For the safeguarding of all involved, users (if permission is granted) must only connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's device.
- The school will take steps to monitor responsible use in accordance with the Responsible Use Policy (Appendix 3).
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.6 Video Conferencing

Video conferencing (including Google Meet, Teams and Zoom) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible should take place using the school's wireless system.

- Staff must refer to the Responsible Use Policy (Appendix 3) prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised appropriately for the pupils' age and ability.

3.8 Cyber Bullying

Cyber bullying can be defined as 'The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone' Dept. For Children, Schools and Families (DCSF) 2007.

- Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's Behaviour, Anti-bullying and Safeguarding and Child Protection policies.

3.9 Data Protection

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

4 Implementation

4.1 Policy in Practice - Pupils

- All users will be informed that network and Internet use will be monitored.
- Online Safety teaching should be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst pupils.
- Online Safety teaching will be included in the PSHE, Citizenship and/or Computing and cover safe use at school and home.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

4.2 Policy in Practice - Staff

- The Online Safety Policy will be provided to and discussed with all members of staff and Responsible User Policy (Appendix 3) signed for compliance.
- Staff should be aware that Internet traffic is monitored and can be 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.

3. Policy in Practice - Parents

- Parents' attention will be drawn to the Online Safety Policy and Responsible User Policy (RUP) in newsletters, Parent Handbook and Website.
- A partnership approach with parents will be encouraged. This could include offering parent evenings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

4. Handling of complaints

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions will be applied depending on the severity of the transgression linked to the school's behaviour policy.