Coloma Convent Girls' School

e-Safety Policy

Approved by:

Board of Governors - 30th April 2018

The e-Safety Policy operates in conjunction with other policies including the Safeguarding Policy, Behaviour & Rewards Policy (including Anti-Bullying Policy) and School Development Plan.

e-Safety Coordinator:	Mrs S. Collins, Deputy Headteacher
e-Safety Representative:	Mrs D. Geoghegan, Designated Child Protection Lead

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

1. Introduction

Usually, the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher. There is therefore a genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- establish the ground rules we have in school for using the Internet;
- describe how these fit into the wider context of our discipline policy;
- demonstrate the methods used to protect the children from sites containing pornography, racist or politically-extreme views and violence.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

At Coloma, we feel that the best recipe for success lies in a combination of site-filtering, supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Parents will be sent an explanatory letter and the rules which form our Internet Access Agreement (attached to the end of this document).

2. Teaching and learning

Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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 enhances learning

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what Internet use is acceptable and what is not and 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.

Coloma ensures that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

Pupils are taught how to evaluate Internet content

Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.

Using the Internet for Education

The benefits include:

- access to a wide variety of educational resources including libraries, art galleries and museums;
- rapid and cost effective world-wide communication;
- gaining an understanding of people and cultures around the globe;
- staff professional development through access to new curriculum materials, expert knowledge and practice;
- exchange of curriculum and administration data with LA/DfE;
- greatly increased skills in literacy, particularly in being able to read and appraise critically and then communicate what is important to others.

The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons.

All staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught and the ICT subject leader will assist in the dissemination of this information.

Initially the pupils may be restricted to sites which have been reviewed and selected for content. They may be given tasks to perform using a specific group of web sites.

Expectations of Pupils using the Internet

Pupils are expected to read and agree the Internet Agreement.

At Coloma School, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site.
- Pupils are expected not to use any inappropriate language in their email communications and contact only people the teacher has approved. They are taught the rules of etiquette in email and are expected to follow them.
- Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.

- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- No programs on data-stick or CD Rom should be brought in from home for use in school. This is for both legal and security reasons.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources. They will also come under the general discipline procedures of the school.

Pupil Evaluation of Internet Content

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy, etc provide an opportunity for pupils to develop skills in evaluating Internet content. For example, researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils use age-appropriate tools to research Internet content.

The evaluation of online materials is a part of teaching and learning in every subject and is viewed as a whole-school requirement across the curriculum.

Managing Information Systems

Coloma recognises the importance of maintaining its Information Systems in relation to security of provision and unauthorised access to ensure the personal safety of staff and pupils.

Coloma subscribes to the following rules in relation to its LAN Network:

- Users must take responsibility for their network use.
- Workstations 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.

Coloma subscribes to the following rules in relation to it Wide Area Network (WAN):

- Central Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools.

- The Schools Broadband network is protected by a cluster of high-performance firewalls. These industry-leading appliances are monitored and maintained by a specialist security command centre.

The security of the school information systems and users will be reviewed regularly and Virus protection will also be updated regularly.

Email management

- All pupils and staff have a network account and individual email address.
- Pupils may only use approved email accounts for school purposes.
- All pupils will be taught how to follow conventions of politeness.
- 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.
- Staff will only use official school provided email accounts to communicate with pupils and parents or carers, as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours or for professional purposes.

How published content is managed

- 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 Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Publishing pupils' images or work

- Images or videos that include pupils will be selected carefully.
- Written or verbal permission from parents or carers will be obtained before images/videos of pupils are electronically published if those images/videos identify individual pupils. Coloma reserves the right to publish images/videos showing groups of pupils without seeking permission where group images do not identify individual pupils by name.
- Pupils' work can only be published with their, or the parents' permission.

Management of social networking, social media and personal publishing

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be alert to the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- 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. 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.

Management of filtering

It is important to recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites).

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.
Teachers should always evaluate any websites 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 ensure that filtering policy is continually reviewed.
- 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 e-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.
- Changes to the school filtering policy will be risk-assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

Protection of Personal data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR May 2018), together with the new Data Protection Act 2018 (DPA 2018).

The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully.
- Processed for specified purposes.
- Adequate, relevant and not excessive.
- Accurate and up-to-date.
- Held no longer than is necessary.
- Processed in line with individual's rights.
- Kept secure.
- Transferred only to other countries with suitable security measures.

Information can only be kept about persons for specific school-related purposes. The information should be kept to a minimum and for as short a period as necessary. It should be removed when the purpose for its use is completed. Users should not have files of any type on any network servers, local hard disks or on the email system that contain information on a person that they would not like that person to see. Any information that users do keep must be of a factual nature and not hearsay.

Any person may, under the provisions of the act, apply to see information about themselves in order to check the accuracy of the content. To delete such information after an application to view is received is an offence under the act.

Users are obliged under the act to take all reasonable steps to minimise unauthorised access to personal information stored on any school computer system. It must therefore be an offence to allow anyone else to use your logon name and password, unless this is specifically for ICT staff to test either your computer or its connection to the network. Never leave any unattended computer logged on for more than a few minutes.

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.

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 or carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, indentify lessons learnt and implement any changes required.

e-Safety complaints procedures

- 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.

Cyberbullying

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
There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular, section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents;
- gives Headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it is investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed, assistance from the police may be sought.

- 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 anti-bullying 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 are clear procedures in place to investigate incidents or allegations of cyberbullying.

Please refer also to Appendix of Coloma's Anti-Bullying Policy

APPENDIX

Internet Agreement

All pupils and their parents or guardians will be asked to read and sign an agreement covering the expectations we have of pupils using the Internet in school.

Coloma School

Dear Parent(s) / Carers,

Responsible Use of the Internet

Pupils have access to the Internet at school. Mindful of the problems there are with children gaining access to undesirable materials, we have taken steps, along with the Local Authority, to deal with this.

Our Internet access has a built-in filtering system that restricts access to sites containing inappropriate content.

All our screens are in public view and an adult is present.

No system is perfect however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material. We have been asked by the LA to inform you of the rules which the pupils are expected to follow to help with our precautions.

I would ask you to look through these rules and discuss them with your child and then return the signed form to us at school.

If you would like to have a look at our full Policy for 'Internet Access', it can be obtained through the office.

Yours sincerely,

ICT Subject Leader

Coloma School Pupil Internet Agreement

This is to be read through with your parent(s) / carers and then signed.

- At Coloma, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Pupils are expected not to use any inappropriate language in their email communications and contact only people the teacher has approved. It is forbidden to be involved in sending chain letters.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on data-stick or CD Rom should be brought in from home for use in school.
- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

I have read through this agreement with my child and agree to these safety restrictions.

To be completed by the parent or carer

PRINT NAME:-______________________ SIGNED:- ________________________

To be completed by the child

PRINT NAME:-______________________ SIGNED:- _______________________

DATE:- ______________________