E- SAFETY POLICY

COLMERS SCHOOL AND SIXTH FORM COLLEGE

Whole School Policy	**E- Safety Policy**
Written by	**Kevin Tranter**
Published	**April 2015**
Reviewed	**June 2017**

Reviewed by Kevin Tranter, Linda Wilcox and Martin Brookes

Date of next review	**June 2018**

Statement of intent

At Colmers School & Sixth Form College, we understand that technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998
- The Regulation of Investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

1.2. This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping Children Safe in Education'

2. Use of the internet

2.1. Colmers School understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools to implement, which minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others

- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert (in accordance with other safeguarding procedures) to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of school and to deal with incidents of such as a priority (see appendix 1).

3.2. The e-safety officer, (Linda Wilcox) is responsible for ensuring the day-to-day e-safety in our school and managing any issues that may arise.

3.3. The headteacher is responsible for ensuring that the e-safety officer and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

3.4. The e-safety officer or designated person will provide all relevant training and advice for members of staff on e-safety.

3.5. The headteacher will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

3.6. The e-safety officer will regularly monitor the provision of e-safety in school and will provide feedback to the headteacher.

3.7. Colmers School has an established procedure for reporting incidents and inappropriate internet use, either by pupils or staff (See appendix 1). All pupil incidents must be logged against pupil behaviour records in SIMS/ MyConcern in the usual way.

3.8. The e-safety officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

3.9. All staff should be aware that all internet access in school, on school systems is monitored and whilst privacy is important, the need to safeguard takes priority. Monitoring of specific staff internet usage will be authorised by the Headteacher, HR or School Business Manager and requests will be logged centrally. Monitoring of specific staff will only be initiated where a need arises in line with existing performance, capability and safeguarding procedures (See appendix 1).

3.10. Cyber bullying incidents will be reported in accordance with the school's Anti-bullying and Harassment Policy.

3.11. The governing body safeguarding committee will hold regular meetings with the e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

3.12. The governing body will evaluate and review this E-safety Policy on a termly and annual basis, taking into account the latest developments in ICT and the feedback from staff/pupils.

3.13. The headteacher will review and amend this policy with the e-safety officer, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

3.14. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.15. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.16. All staff and pupils will ensure they understand and adhere to our Acceptable Use Policy, which they must sign and return to the headteacher.

3.17. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

3.18. Colmers School will ensure regular communication with parents and update them on current e-safety issues and control measures (See appendices 2, 4 and 5).

4. E-safety control measures

4.1. Educating pupils:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of school.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all IT classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- Use of mobile devices in school will be in line with the published Mobile Devices policy.
- E- Safety updates and assemblies will be delivered at appropriate times throughout the year.

4.2. Educating staff:

- All staff will undergo e-safety training on an annual basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.
- All staff will undergo regular audits by the e-safety officer in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.

4.3. Internet access:

Internet access will be authorised once parents and pupils have returned the signed consent form as part of our Acceptable Use Policy.

A record will be kept by the headteacher of all pupils who have been granted internet access.

All users will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other pupils using their login details.

Pupils' passwords will be changed on a regular basis, and their activity is continuously monitored by the e-safety officer.

Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

Effective filtering systems will be established to eradicate any potential risks to pupils through access to particular websites.

The E- Safety referral system will be followed by the appropriate staff when breaches have been made by students (see appendices 3, 4 and 5).

Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the E-Safety lead, or a member of SLT.

All school systems will be protected by up-to-date virus software.

An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

Regular monitoring of activity will be available to the headteacher to review.

Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

Personal use is monitored in the same way as other use, however the log will only be reviewed by the Headteacher for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and no personal devices. This will be dealt with following the process outlined in section 6.2 of this policy – 'misuse by staff'.

4.4. Email:

- Pupils and staff will be given approved email accounts and are only able to use these accounts.
- Use of personal email to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

4.5. Social networking:

- Use of social media on behalf of the school will be conducted following the processes outlined in our Social Media Policy.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.
- Pupils are regularly educated on the implications of posting personal data online, outside of school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

4.6. Published content on the school website and images:

- The headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the school website will be the phone, email and address of the school. No personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

4.7. Mobile devices and hand-held computers:

Please refer to the detailed Mobile Devices Policy:

- Staff may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use, or educational use
- Mobile devices are not permitted to be used during school hours outside lessons by pupils.
- Staff are permitted to use hand-held computers which have been provided by school, though internet access will be monitored for any inappropriate use by the e-safety officer when using these on the school premises.

- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices must not be used to take images or videos of pupils or staff.
- Colmers School will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.
- The E- Safety referral system will be followed by the appropriate staff when breaches have been made (see appendices 3, 4 and 5).

4.8. Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the IT Support Team.
- The IT Operations Manager must ensure that the filtering of websites and downloads is up-to-date and monitored.

5. Cyber bullying

5.1. For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

5.2. Colmers School recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

5.3. Colmers School will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

5.4. Colmers School will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

5.5. Colmers School has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-bullying and Harassment Policy.

5.6. The headteacher or DSP will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

6. Reporting misuse

6.1. Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the pastoral team.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the pastoral team and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection Policy.

6.2. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the Headteacher.
- The headteacher will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

APPENDICES:

APPENDIX ONE: Safeguarding: E- Safety organisation map.

APPENDIX TWO: Whole school E- Safety letter.

APPENDIX THREE: E- Safety Referral policy and procedure.

APPENDIX FOUR: Referral letter one.

APPENDIX FIVE: Referral letter two.

Safeguarding: E-Safety…

APPENDIX ONE

Key:

School systems used | Key Staff | Key Documents

What is E-Safety?

This can also be called '**internet safety**', 'online **safety**' or 'web **safety**'. **E-safety** is often **defined** as the **safe** and responsible use of technology. This includes the use of the **internet** and also other means of communication using electronic media (e.g. text messages, gaming devices, email).

360safe
the e-safety self review tool

School monitoring systems:
SMOOTHWALL filtering software

K Tranter
School Business Manager
(ext. 2066)
Monitors Kevin Whiley for malpractice

K Whiley
IT Operations Manager
(ext. 2153)
Monitors students and staff for malpractice

M Brookes
Assistant Headteacher
DSL
(ext. 2045)
Audits systems each term.
Informed of any immediate CP issues by Kevin Whiley

Assistant Headteacher for Behaviour/ Heads of Year/ PSW

L Wilcox, D Hodgson, I Queen, P Bradley, R Ramsey, A Bennett, T Charlett

Investigate and sanction children following the ***E-Safety referral policy and procedure.*** This may include but is not exclusive to: Interviewing the child, calling parents, writing to parents, sanctioning the child and removing access to any computers or methods of accessing the internet in school.

KEY DOCUMENTATION

E- Safety policy 2017-18

Data protection policy 2016/17

Mobile phones and devices policy 2016/17

ICT acceptable use policy 2016/17

Staff Code of Conduct policy 2016/17

COLMERS SCHOOL
& SIXTH FORM COLLEGE

APPENDIX TWO

Dear parents/carers,

As you will of course be aware, technology plays a greater role in all our day to day lives. Pupils have greater access to a whole world of information at their fingertips. It is hoped that this access can lead to a greater thirst for knowledge and progress across a range of subjects. Pupils will also have the ability to develop and improve their understanding beyond the classroom environment. As such, at Colmers we invest a considerable amount of resources in enabling pupils to access technology through wired and wireless means.

The vast majority of pupils make good use of this access and find considerable benefit from what is on offer at Colmers, and operate well with the expectations of the Acceptable User Policy, which all agree to on signing in to any device.

However, we are aware that on occasions pupils will make the wrong choices. This may result in pupils using the equipment inappropriately or in pupils accessing inappropriate material. Safeguards are in place with regards to this and we have software that alerts of inappropriate access, including blocking the site and providing a notification to our IT Support Team. Issues arising will then be discussed with pupils and access withdrawn for periods of time if required.

We have had recent situations where pupils are accessing content outside school using mobile devices and then come into school with the same content on their device. Where pupils have then accessing the school Wi-Fi system this has created an alert as the web sites have refreshed. We would encourage appropriate use of IT at all times and thank you for your support in helping to ensure pupils learn effective life skills and stay safe in an increasingly on line world.

As always, should you have any thoughts or questions please feel free to contact the school.

Regards

M Brookes

Assistant Headteacher

Designated Safeguarding Lead

L Wilcox

Assistant Headteacher

APPENDIX THREE:

Colmers School and Sixth Form College

E-Safety Referral Policy and Procedure

COLMERS SCHOOL
& SIXTH FORM COLLEGE

360 safe
the e-safety self review tool

In all instances where you suspect a Child Protection issue you must inform ***M Brookes (DSL)*** on ***2045*** or ***L Wilson (DDSL)*** on ***2171*** immediately.

STEP 1

Student breaches Colmers School E-Safety policy for the first time.

Actions:

Parents are informed of the breach by HOY if deemed necessary.

Student is warned regarding future conduct.

STEP 2

Second breach of school E-Safety policy. Log on MyConcern

Actions:

Parents are informed of the breach by HOY via phone call.

Student is given a one hour Senior Leadership Detention.

STEP 3

Third breach of school E-Safety policy. Log on MyConcern

Actions: Use letter one.

Parents are notified by letter. Meeting arranged with HOY and LW.

Child is banned for a short term fixed period. E Safety education plan is put in place.

STEP 4

Fourth breach of school E-Safety policy. Log on MyConcern

Actions: Use letter two.

Parents are notified of the situation. Meeting arranged.

Child is banned from using any internet/ messaging devices in school.

Referral to outside agencies regarding E-Safety is made.

APPENDIX FOUR:

Dear parents/carer,

As you are aware, through previous discussions, in the past year your child has breached the E-Safety policy of the school and has been flagged on two occasions for inappropriate internet use. Unfortunately I am writing to inform you that a third breach has taken place. As a result of this we would like you to attend a meeting in school to discuss this matter further.

School policy dictates that your child will be banned from all use of the internet and Wi-Fi on school premises for a fixed term period to be determined at the meeting. However, the most important part of the meeting will be to discuss an E-Safety education plan for your child. We at Colmers want to support your child to make the right choices and keep themselves safe online. We are also happy to support you in being able to monitor your child's online activity and set up appropriate settings on any devices if required.

The safety of your child is of paramount importance to us. I hope that by working together to support your child we can ensure that incidents of this nature do not happen again.

Please contact the school to arrange a meeting at your convenience. If you wish to discuss any of the content of this letter prior to the meeting feel free to contact the school.

Regards

M Brookes

Assistant Headteacher

Designated Safeguarding Lead

L Wilcox

Assistant Headteacher

APPENDIX FIVE:

Dear parents/carer,

Thank you for your support regarding the recent E Safety issues we have had with XXXXXXX. We were hoping that the interventions that we had put in place between us would have had a significant impact on your child being able to safeguard themselves online. Unfortunately this has not been the case as we have been alerted of another E Safety breach in school. As a result of this we would like you to attend a meeting in school to discuss this matter further.

School policy dictates that your child will be banned from all use of the internet and Wi-Fi on school premises until further notice. However, the most important part of the meeting will be to discuss an E-Safety education plan for your child. Despite our best efforts the school based interventions that have been put in place have not been effective. Therefore, we need to discuss the appropriate solutions available that can be provided by external agencies.

The safety of your child is of paramount importance to us. I hope that by working together to support your child we can ensure that incidents of this nature do not happen again.

Please contact the school to arrange a meeting at your convenience. If you wish to discuss any of the content of this letter prior to the meeting feel free to contact the school.

Regards

M Brookes

Assistant Headteacher

Designated Safeguarding Lead

L Wilcox

Assistant Headteacher