Churchill Community College
E-Safety Policy

Background

E-Safety encompasses the use of new technologies, internet and electronic communications, publishing and the appropriate use of personal data. E safety is the ability to protect and educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The College's E-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security and our Acceptable Use Policy.

This policy applies to:	All Staff, Students, Governors and Visitors
This policy comes into effect:	September 2008
The policy was reviewed:	March 2013, October 2013, Nov 2014, Sept 2015

Research has proven that use of technology brings enormous benefits to student achievement, learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings

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

- Responsible ICT use by all staff and students and made explicit through published policies.
- Sound implementation of E-safety policy in both administration and curriculum, including secure College network design and use.
- Safe and secure broadband and wifi access including the effective management of filtering across all devices

CONTENTS PAGE

SECTION 1 - E SAFETY TRAINING AND PRACTICES

STAFF

- Whole staff training takes place annually
- The College operates a managed system
- The Designated Child Protection Coordinator is the Head Teacher
- Internet access is provided by an approved educational Internet service provider and complies with DFE requirements for safe and secure access.
- The College filtering policy has been approved by the LT
- An ICT security audit has been initiated by LT, possibly using external expertise.
- College personal data is collected, stored and used according to the principles of the Data Protection Act.
- Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of LT. On a day to day basis they are supervised by the Curriculum Leader for ICT
- Workshops to raise awareness of Prevent are delivered to all staff
- Key staff (Designated Person and Learning Coordinators) attend training on Child Sexual Exploitation.

PARENTS

- Students and parents were involved in the development of this e safety policy. The E safety policy is regularly reviewed and updated.
- Information about e safety is shared on the college website about e safety e.g. advice on how to deal with cyberbullying.

STUDENTS

- There is an assembly programme which covers e safety issues e.g. cyber bullying. This is followed up with work in tutor time at specific times of the year.
- Rules for Responsible Use have been set for students and there is annual training for students about the appropriate use of the college network and what to do if an issue arises e.g. they are able to access an inappropriate website
- E safety is covered as part of the PSHCE programme and is age appropriate. This is delivered by CEOP trained teachers.
- There are robust reporting channels by which issues are reported, including concerns about radicalisation.

- There are a number of members of staff who work together to maintain e safety in the College (Assistant Head, Head of ICT, Senior ICT technician, Guidance Team, Strategic lead for Prevent) and there are four CEOP trained ambassadors.

SECTION 2 - VISION FOR E SAFETY

- To provide a diverse, balanced and relevant approach to the use of Technology
- To encourage students to maximise the benefits and opportunities that technology has to offer
- To ensure that students learn in an environment where security measures are balanced appropriately with the need to learn effectively
- To equip students with the skills and knowledge to use technology appropriately and responsibly
- To teach students how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- To ensure that all users in the College community understand why there is a need for an eSafety Policy

eSafety Champion

The eSafety Champion is the Assistant Head - Guidance

The role of the eSafety Champion includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Keeping personally up-to-date with eSafety issues and guidance through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP) and Prevent Duty Guidance.
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

SECTION 3 - 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 College 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 students.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

Internet use will enhance learning

- Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment in order to enrich and extend learning activities.
- The College Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

- The College will ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students use the Internet widely outside College and will need to learn how to evaluate Internet information and to take care of their own safety and security.

SECTION 4 - MANAGING INTERNET ACCESS

Information system security

- College ICT systems capacity and security will be reviewed regularly as part of the annual audit.
- Virus protection will be installed and updated regularly by the Technical Support Team (TST)
- Security strategies will be discussed with the Local Authority.

E-mail

Staff and students must understand that the use of the College network is a privilege which can be removed should reason arise. The College may monitor all network and Internet use in order to ensure student safety.

- Staff and students may only use approved e-mail accounts on the College system.
- Students must immediately tell a member of staff if they receive offensive e-mail. Staff should notify their link member of the LT and the Learning Coordinator. Issues will be passed onto the ntlp who will work with the college to resolve it.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on College headed paper.

Published content and the College web site

- The contact details on the Web site should be the College address, e-mail and telephone number. Staff or students' personal information will not be published.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Social networking and personal publishing

- The College will block/filter access to known social networking sites.
- Forums will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location. Where students need to create used accounts they will be instructed to use their ntlp e mail addresses.
- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications whilst using social networking sites at home. Students should be encouraged to invite known friends only and deny access to others. (PLEASE SEE SECTION ON CYBER BULLYING)

Managing filtering

- The College will work in partnership with North Tyneside Council and other agencies to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site e.g. promoting extremist views or showing inappropriate images, it will be reported to the Technical Support Team or Head of ICT.
- In conjunction with NTC we will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

ACCEPTABLE USE POLICY

Authorising Internet access

- All staff will read and sign the 'Acceptable Use Policy' before using any College ICT resource.
- The College will maintain a current record of all staff and students who are granted access to College ICT systems.

Assessing risks

- The College will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a College computer. Neither the College nor NTC can accept liability for the material accessed, or any consequences of Internet access.
- The College will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a member of LT.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with College child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with NTC and the Police to establish procedures for handling potentially illegal issues.

COMMUNICATIONS POLICY

Introducing the E-safety policy to students

- Students will be informed that network and Internet use will be monitored.

Staff and the E-Safety policy

- All staff will be given the College e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management/ curriculum leader ICT and have clear procedures for reporting issues.

Enlisting parents' support

The College will inform parents that students will be provided with supervised Internet access. Parents'/Carers' attention will be drawn to the College E-Safety Policy on the College Web site.

Internet safety

Students will be educated in the responsible and safe use of the Internet and other technologies through a range of strategies including:

- ICT lessons in KS3
- The Think U Know training materials
- The Becta leaflet 'Signposts to Safety'
- Reactive discussion when suitable opportunities occur e.g. discussing sensitive topics such as sexual exploitation, terrorism and extremism ideas, and how to challenge these

SECTION 5 - USE OF MOBILE DEVICES

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

MOBILE PHONE POLICY

Students are allowed to bring mobiles phones into College but must follow these guidelines:

- Mobile phones MUST be switched OFF during lesson time so they cause NO disruption to learning.
- Mobile phones should NOT be used in lessons (phonecalls, texts, messages, Snapchat, accessing internet e.g. Facebook, listening to music, taking photographs or videos) unless the teacher has given clear permission as part of the lesson (e.g. calculator use, music used for a dance lesson)
- In a lesson, if a student is seen with a phone or a phone is heard, they will be asked to put it away and name put on board as part of behaviour system. Phones will be taken if students check their phone for received messages or phones make any noise – they need to be switched off. If it is seen again, it will be confiscated by the teacher, in most cases until the end of the lesson.
- Phones may be taken for longer or referred to a Learning Coordinator if a student is regularly not following the rules. The member of staff will make the final decision about confiscating phones and it may be until the end of the week.
- The Learning Coordinators will monitor students who are constantly having their phone confiscated and disrupting learning. They will contact parents and agree sanctions with parents e.g. their mobile will not be allowed in school.
- AT NO TIME should phones be used to take photographs or videos in school – this includes all social times e.g. break and lunch.
- The sending of abusive or inappropriate messages is forbidden.

CONTACTING STUDENTS DURING THE SCHOOL DAY

In line with Churchill's safeguarding procedures, parents should contact students through the main reception / switchboard e.g. if a parent needs to get an urgent message to a student.

If a child contacts a parent to say they are feeling ill or upset, the parent should contact the main school reception in order that we can investigate further and then get back to them with more information. A child may not have informed staff about the concern and therefore

we would not be able to support the student effectively, unless we have communication from the parent.

If a parent arrives at reception without having called the College to set up a meeting, we cannot guarantee that they will be able to speak to the member of staff they want to see.

We expect students to have phones turned off during lesson time, so if you needed to contact your child urgently, you would need to follow the procedures listed above and not assume they would receive a message on their mobile.

SECTION 6 - USE OF DIGITAL MEDIA

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

Publishing student's images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the College Web site.
- Work can only be published with the permission of the student and parents.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son. We follow the following rules for any external use of digital images:

- If the pupil is named, we avoid using their photograph.
- If their photograph is used, we avoid naming the pupil.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film. Only images of pupils in suitable dress are used.

Examples of how digital photography and video may be used at school include:

- Your child's image being used for presentation purposes around the school;

e.g. in class or wider school wall displays or PowerPoint presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

SECTION 7 - THE USE OF SOCIAL NETWORKING AND ON-LINE MEDIA

This College asks its whole community to promote this approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic, extremist or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse or extremist views - initial abusive messages should be saved as evidence before blocking the sender.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

COLLEGE PRACTICE

The college uses social networking sites to share information with students and parents e.g. Churchill Community College facebook site, Art department facebook site, PE department twitter page, etc. These sites are authorised by the college in advance of use and are therefore closely regulated according to our social networking policy.

STAFF PRACTICE

- Staff will not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- The only digital communication between staff and students should be on the College e mail or College approved social media sites.
- If staff use Social Network sites, details will not be shared with pupils and privacy settings will be set at maximum.
- Students will not be added as 'friends' by staff on any Social Media sites. Staff will decline all 'friend' requests from students.
- Staff will always conduct themselves in a professional manner.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the police and /or dealt with by the College behaviour policy. *(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)*

The whole school community is reminded of the CEOP report abuse process: https://www.thinkuknow.co.uk/parents/browser-safety/

SECTION 8 – SOCIAL MEDIA
CYBER BULLYING, EXTREMISM AND E SAFETY ADVICE FOR STUDENTS AND PARENTS

Research shows that currently 3% of 5 -7 year olds have a smartphone and 35% age 12 – 15yrs.

Social networking sites e.g. Facebook, Twitter, are an important part of the social lives of young people today. Unfortunately, they can also be used negatively e.g. to bully others.

Churchill Community College would like to offer the following guidelines to students and parents to make sure the use of these sites is enjoyable and safe. The majority of use takes place outside of school and so must be managed by parents effectively to avoid problems occurring.

IF BULLYING OR OTHER PROBLEMS OCCUR ON SOCIAL MEDIA

AS A PARENT YOU SHOULD:

- Report the bullying to the service provider and to the police.
- Keep evidence e.g. the text message or print out from Facebook.
- Block or delete the person who has bullied.
- Change the phone number.
- Check the security settings and privacy settings on your child's account. These need to be updated regularly.
- Monitor your child's use of the internet, social networking and gaming sites e.g. review their friends list – do they know who all these people are? You would warn them against talking to strangers on the street so exactly the same rules apply on line.
- Make sure that your child is careful about who they give their BB pin to. In being part of a group your child might receive unwanted messages, images or videos
- Your child must tell a parent or teacher immediately if they receive an inappropriate image, video (e.g. of a fight taking place) or extremist material. If they just store it on their phone or computer, or even open it and delete it, they could find themselves in trouble with the police at a later date, even if they did not ask for that image to be sent to them. The key message is to tell an adult straight away and not pretend it did not happen.

- Make sure that your child understands that information put online stays there forever. Deleting a message on your computer does not mean that it cannot be recovered by someone else at another time
- Ensure that children under 13 do not have Facebook accounts

Please do not involve yourself in the dispute by sending a message yourself as you could then find yourself in trouble as well. Instead report it to Facebook/ Twitter and the police.

Useful information on e safety can be found on:

- CEOP's youtube channel - http://www.youtube.com/user/ceop?feature=chclk.
- Vodafone's digital parenting site http://www.vodafone.com/content/index/parents.html - this is full of great resources like advice on parental controls, checking privacy settings with your children, check lists for things to be aware of for different age groups of children and a great digital magazine on all the issues in this area.
- The UK Safer internet centre also has a parent's guide to technology - http://www.saferinternet.org.uk/advice-and-resources/a-parents-guide
- CEOP - www.thinkuknow.co.uk
- BBC Stay Safe site
- Sophos

AS A COLLEGE WE WILL:

- Record all bullying incidents, including cyber bullying
- Recommend that you de-activate social media accounts
- Investigate any issues that are brought to our attention. As part of this we may ask students and parents to give evidence of the comments made e.g. print out of Facebook comments or we might ask to read a text. Please do not delete these messages.
- Once an investigation is complete, students proved to be involved in bullying will be sanctioned in line with our behaviour policy e.g. internally excluded or receive an internet ban on the College network.
- Involve the police if necessary

STUDENTS SHOULD:

- Use social media responsibly e.g. do not make rude, abusive or threatening comments to anyone.
- Only talk to people they know and only accept people they know as friends. They should not give out personal information e.g. address, phone number, e mail address. The same applies to people they may play games against online. They should be very careful about what images / videos of themselves that they post on line.
- NEVER go and meet anyone they have met online, Lauren who is 15 could turn out to be Rob who is 45.
- Be careful about who they give your BB pin to. In being part of a group your child might receive unwanted messages, images or videos
- NEVER share passwords
- NEVER download information illegally e.g. music
- Be aware that comments made online or pictures posted are there forever. Deleting a message or image on your computer does not mean that it cannot be recovered by someone else at another time.
- Be aware that friends of friends may be able to see comments, photo's etc because of their privacy settings.
- Check the security settings and privacy settings on their account. These need to be updated regularly.
- Tell a parent or a member of staff if they are bullied online or text, or receive extremist material.
- MUST tell a parent or another adult immediately if they receive an inappropriate image or video (e.g. of a fight taking place) they just store it on their phone or computer, or even open it and delete it, they could find themselves in trouble with the police at a later date, even if they did not ask for that image to be sent to you e.g. you receive through BB.
- Report any bullying to Facebook / Twitter but keep the evidence.
- Block or delete the person who has bullied or shared inappropriate material.

REMEMBER – NO INFORMATION IS 100% PRIVATE ONCE YOU PUT IT ON SOCIAL MEDIA.