



CANNOCK CHASE HIGH SCHOOL

A C H I E V E M E N T F O R A L L

E-SAFETY POLICY

This policy **MUST** be read in conjunction with Cannock Chase High School Safeguarding Policy, Behaviour Policy, ICT Acceptable Usage Rules, Staff Acceptable ICT Usage Policy and our Anti-bullying Policy.

What is E Safety?

Cannock Chase High School believes that the use of information and communication technology in school brings great benefits. This Policy aims to recognise e-safety issues and will help to ensure the appropriate, effective and safer use of electronic communications for all students and staff.

We are aware that in today's society children, young people and adults interact with technologies such as; mobile devices (including phones, tablets, wearable technology e.g. smart watches), games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved can be greatly beneficial to all, but can also place children in danger.

This E-Safety Policy covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communication technologies, **both in and out of school.**

Aims of the E-Safety Policy

- To safeguard children, young people and staff.
- To be able to identify the risks associated with social networking.
- To identify roles and responsibilities and recognise that e-safety is part of the 'duty of care' which applies to everyone working with children.
- To educate and empower children so that they possess the necessary skills to make safe and responsible decisions and to feel confident to report any concerns they may have.
- To raise awareness of the importance of e-safety amongst all staff so they are able to educate and protect children in their care.
- To inform staff how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.
- To provide opportunities for parents/carers to develop their knowledge of e-safety.

Important Information

All students will be expected to read our Rules for Acceptable ICT Usage and sign the appropriate consent documentation before an account is created and maintained. (See Appendix 1).

Parents/carers of students in Key Stage 3 and 4 will be asked to discuss our Rules for Acceptable ICT Usage with their child, where appropriate.

Further staff guidance for personal use and social networking will be discussed as part of staff induction and safe and acceptable professional behaviour will be outlined in the Staff Acceptable Use policy.

Cannock Chase High School will ensure that:

The E-Safety Policy will be reviewed annually.

A member of the Senior Leadership team has responsibility for e-safety in school.

The school appoints a member of the Governing Body to take lead responsibility for e-safety.

A member of school staff will be accredited with CEOP (Child Exploitation and Online Protection) training.

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).

The Designated Safeguarding Officer will be informed of any e-safety incidents involving safeguarding concerns, which will then be acted on appropriately.

The school will manage e-safety incidents in accordance with the school's Behaviour and Anti-Bullying Policies where appropriate.

The school will inform parents/carers of any incidents of concern as and when required.

Where there is a cause for concern or fear that illegal activity has taken place or is taking place, then the school will contact Staffordshire Children's Board Safeguarding Team for advice and/or escalate the concern to the Police. The Police will be contacted if a criminal offence is suspected.

Any complaint about staff misuse must be directly reported to the Headteacher (See Staff Acceptable ICT Usage Policy). We work in partnership with Parents/Carers and students to resolve issues. Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and Safeguarding procedures. All members of the school community will be reminded about safe and appropriate behaviour online and the importance of **not** posting any content, comments, images or videos online **which cause harm, distress or offence to any other members of the school community**

Cyber Bullying

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.

Many children, young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively and we have a duty to safeguard all students and staff.

When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone. This can be harmful, threatening and a great source of anxiety. Where bullying outside school (such as online or via text message/voicemail) is reported to school, it will be investigated and acted on.

Cannock Chase High School will ensure that:

Cyberbullying (along with all other forms of bullying) of any member of the school will NOT be tolerated.

There are clear procedures in place to support anyone in the school community affected by Cyberbullying.

There are clear procedures in place to investigate incidents or allegations of Cyberbullying (see Anti-Bullying Policy).

Mobile Phone Procedures

Students (including Sixth Formers) at Cannock Chase High School are only allowed to use their mobile phones at break and lunch times. Phones will be confiscated at any other times and passed to the relevant Director of Year/Pastoral Manager. On the third occasion a mobile phone is confiscated a parent is required to come into school to collect the mobile phone.

Where a student/member of staff believes that a mobile phone may have been used inappropriately during the school day to record/take pictures of staff and/or students they must report this incident to Directors of Year/Senior Leadership for investigation.

Where a member of staff believes that a mobile phone has 'inappropriate' material/images on the phone they must report this incident to Directors of Year/Senior Leaders for investigation.

The school reserves the right to confiscate and retain mobile phones if there is evidence to believe 'inappropriate' material/images are on the phone. The school will then decide on the most appropriate form of action under each individual set of circumstances with Safeguarding and keeping students safe at the heart of our decisions.

Roles and Responsibilities of Members of our School Community

Students and Staff MUST:

Report immediately, to a **designated member of staff**, if they receive offensive or abusive e-mails, text messages or posts on social networking sites.

Report immediately, to a **designated member of staff**, if they have information that another member of the school community has experienced any of the above.

Not reveal personal details of themselves or others which may identify them and/or their location.

Set passwords to their accounts in and out of school.

Deny access to unknown individuals and block unwanted communications on social network sites.

Not publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Follow Cannock Chase High School's 'Top Tips for e-safety'.

Communicating E-Safety

E-safety information leaflet for students, parents and carers is available on the school website.

Providing 'cyberbullying' government guidance for parents on the school website.

E-safety posters with students' '*Top Tips*' for keeping safe when using the Internet will be displayed in all Form Tutor rooms, ICT rooms and Pastoral Offices. (Appendix 2)

An e-safety training programme will be established across the school to raise the awareness and importance of safe and responsible Internet use amongst students.

Regular training (CPD Continuing Professional Development) will be provided for all staff by external agencies, raising awareness of technological and social issues related to e-safety.

An e-safety module will be delivered through PSHE, covering both safe school and home use at times throughout the year.

The E-Safety Policy will be discussed with all members of staff and displayed on our school website.

To protect all students and staff, the school will implement Rules for Acceptable ICT Usage.

Parents' attention will be drawn to the school's E-Safety Policy, e-safety leaflet and e-safety awareness video in newsletters, other communications and on the school website.

A partnership approach to e-safety at home and at school with parents will be encouraged by offering parental e-safety sessions in partnership with relevant external agencies.

Subject staff are encouraged to discuss, advise and take the opportunity to give e-safety reminders when using ICT in lessons.

E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk . Alternatively, follow the link on our school website.

Useful e-safety programmes include:

Think U Know: www.thinkuknow.co.uk

Childnet: www.childnet.com

Kidsmart: www.kidsmart.org.uk

Review Date: December 2018



RULES FOR RESPONSIBLE ICT USAGE

Name of Student: _____

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only access the system with my own login and password, which I will keep secret.
- I will only access areas of the schools FROG VLE system that I am allowed to and will use all areas responsibly.
- I will not access other people's files.
- I will only use the computers for school and homework.
- I will ask permission from a member of staff before using the Internet.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give my home address or telephone number, or arrange to meet someone unless my parent, carer or teacher has given permission.
- I will report any unpleasant material or messages sent to me to my teacher or Director of Year.
- I will not attempt to access social media sites such as Facebook, Instagram from any school computer.
- I understand that the school may check my computer files and may monitor the Internet sites I visit as part of Safeguarding Procedures.
- I am aware that should I be involved in the misuse of the school's computer system I may have my computer and internet privileges removed or face more serious sanctions including fixed and permanent exclusion if engaged with events that breach the school's disciplinary procedures.

Signed: _____

Date: _____

Appendix B

Cannock Chase High School's Top Tips for E-Safety

- 1) Do not add people that you don't know on social networking sites. You would not talk to a stranger in the street, so why talk to them online?
- 2) Do not upload photographs of yourself that are inappropriate or give information away about yourself. You don't know how these images will be used by others.
- 3) Do not give away your personal details on the internet. You don't know who can access this information.

If you feel unsafe online, tell a parent, carer or teacher.