Chiltern Way Academy Trust

Turning Futures Around

Student
E-Safety Policy

Responsibility for this policy (job title): IT Manager

Responsibility for its review: CEO

Approved: 04/05/2023

Next Review Date: Summer 2024

CONTENTS

Purpose

The use of new technologies is evident in all areas of modern life, we recognise the importance of technology in enhancing education but acknowledge that there are many potential difficulties for both staff and students.

This policy has been written to complement the Academy's Safeguarding Policy and Behaviour Policy.

The relevance of this policy will be monitored on a regular basis, and the policy will be updated annually to accommodate technology and system developments.

Applicability

This policy applies to all Chiltern Way Academy Trust (CWAT) students.

Roles and Responsibilities

The Heads of Campus are responsible for ensuring that all Academy students, parents/carers and staff are made aware of the E-safety Policy. Heads of Campus are also responsible for making sure that this policy is adhered to.

Breaches of this policy may lead to actions as outlined in the Academy's Behaviour Policy and Safeguarding Policy. External agencies, such as the Police and Children's Services, will be involved when necessary.

Protecting Students

All students are expected to abide by the acceptable use policy when using CWAT Information Computer Technologies resources (Appendix 1).

Leavers

- When a student leaves CWAT, their access to all CWAT computer equipment and systems will be suspended immediately.

Passwords

- All student passwords are set and provided by the school. If a password is believed to have been compromised, the IT support team must be informed immediately. Students are responsible for ensuring that only they have access to their computer account.

Internet Filtering

The CWAT Internet connection is fully monitored and protected by Firewalls to ensure student browsing is protected as much as is possible.

- CWAT uses an internet monitoring and filtering system called Smoothwall which is reviewed by the Academy Lead Safeguarding, Welfare and Attendance Manager on a regular basis.
- The Smoothwall software forensically monitors students' internet use. Smoothwall identifies online use which could indicate a vulnerable person, bullying/violence, sexual content, an offensive user, over sharing, grooming, terrorism/extremism and general risk. Smoothwall sends a real-time alert which can be dealt with in a timely manner by the Campus Safeguarding Welfare and Attendance Manager who may delegate to a member of the Support Team where this is considered to be the most appropriate action.
- We also have SonicWall firewalls in place that have various restrictions for web access.

Communication Enabled Devices

CWAT does not allow students to bring communication-enabled devices, such as smartphones into the Academy (see Behaviour Policy). Students who arrive at school with a device are requested to hand it in to be held securely until the end of the day at which time they can collect it. However, if students have signed the mobile phone contract confirming they understand how to behave appropriately online there are some circumstances when they may be given access to it e.g. to support them on a long journey. Students are aware that, should they behave inappropriately, this privilege will be withdrawn from them.

We acknowledge that students use their devices to maintain contact with each other and use messaging and social media applications, such as WhatsApp, Snapchat and TikTok. There are a number of difficulties that can arise from the use of social media applications, specifically the ability to broadcast text, images or film quickly. We will encourage students to think carefully about the use of these applications and will support families should difficulties arise (see Safeguarding Policy).

Using the Internet

- As stated in the Internet Filtering section above, students should be aware that the internet at the Academy is provided for educational purposes and that the Academy maintains logs of their internet use. Students should feel confident in reporting internet content that makes them feel uncomfortable. Support will be offered to any student who has encountered uncomfortable content.

- Sanctions will not be applied to any student reporting inappropriate content, provided that internet logs do not show active searching for inappropriate material.

- Students should be made aware of the existence of inappropriate websites so that they understand the dangers of material on these, however they should never be directed towards these. These include websites that contain inappropriate material such as pornography, violence, unhealthy lifestyle promotion e.g. anorexia, bulimia, hate material e.g. racist, sexist, homophobic messages etc...

Cyber Bullying

- Students need to be made aware the Academy will treat cyber bullying with the same severity as any other form of bullying.

- Students will be encouraged to report any form of online interaction that has made them feel upset. Incidents will be dealt with under the Academy's Behaviour Policy and Safeguarding Policy, as appropriate.

- Students should, where possible, retain evidence of the interaction(s) and be encouraged not to respond, but instead to report it.

Sharing Personal Information and Content

- Students need to understand that new technologies allow the instant sharing of content with a wide range of people. Before publishing content, students should pause to consider the reasons why they want to publish the content, and the potential implications of doing so.

- Students need to be aware of the dangers of sharing their personal information/content online.

- Specific situations should be highlighted with appropriate examples of the dangers these situations can pose:

➢ Grooming – Making friends online can help people meet others with common interests and ideas. There are many examples of positive online friendships, however sharing too much information can highlight vulnerabilities and these can be exploited. Students should think carefully about these online friendships and be able to satisfy some simple questions such as: Do I really know what this person looks like? Can I be sure this person is who they say they are? Why do they want to be my friend? Students will be warned never to meet anyone they have only met online without talking first to their parent/carer.

➢ Nudes and semi-nudes –Modern technologies allow people to share images and video easily. Students need to be aware that creating, possessing and/or sharing indecent images of children is a criminal offence. When an image is shared the subject immediately loses all control over that image as it can then be shared with many other people without their consent.

➢ Digital footprint – Various online forums and social networking websites enable people to have a platform for their thoughts. These sites maintain archives of posts for many years and can be easily searched. Students will be made aware that when posting online content, it forms part of their digital footprint that can be accessed by anyone. They should think carefully about what they are posting, and whether it is something they would feel comfortable discussing in an open forum. Students should also ensure that they know how to maintain the security settings on their social networking sites to maintain their privacy.

- Copyright – A huge variety of content is freely available online. This content can be used to enhance and improve learning. Students will be made aware that they must check the source of online material that they use. Sources must be accredited, and copyright law respected. The use of ChatGPT or other AI-derived content must always be acknowledged by students. Plagiarism of online content will be dealt with under the Academy's Behaviour policy.

Event Recording and Monitoring

- Incidents of breaches of the E-safety Policy by students will be recorded by a member of staff on CPOMS and dealt with in line with both the Behaviour Policy and Safeguarding Policy.

APPENDIX 1: Student Acceptable Use Contract

Covers use of digital technologies in Chiltern Way Academy Trust (CWAT): email; internet; intranet and network resources; learning platform; software, equipment and systems.

ICT systems, technologies and software are made available to students to further their education.

This Acceptable Use Contract has been drawn up to protect students, staff and the Academy. The Academy reserves the right to examine or delete any files that may be held on its computer systems, and to monitor all internet use/ work completed by a user.

I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety, or to the safety and security of the ICT systems and other users. All students using CWAT provided computer equipment automatically agree to the following rules:

For my own personal safety

- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications. This will include monitoring and accessing any personal area on the network, such as My Documents.

- I understand that the Academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so. I will only use the Academy's computers for Academy work, homework and as directed.

- I will not bring files into the Academy (on removable media or online) without permission, or upload inappropriate material to my workspace.

- I will only edit or delete my own files and not view, or change, other people's files without their permission.

- I will keep my logins, usernames and passwords secret; I will not share these, nor will I try to use any other person's username and password.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not use the Academy ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting.

- I will use the Internet responsibly and will not visit websites I know to be banned by the Academy. I am also aware that during lessons I will only visit websites that are appropriate for my studies.

- When I am using ICT resources, I will act as I expect others to act toward me.
- I will respect others' work and property and will not access, copy, remove, or in any way alter, other users' files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others; nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place.
- I will immediately report to a trusted adult any unpleasant or inappropriate material, messages or anything that makes me feel uncomfortable when I see it online.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share personal information (my home address, phone number, photographs or video, or give any other personal information that could be used to identify me or my family or my friends, unless a trusted adult has given permission) about myself or others when on-line.
- I will never arrange to meet someone I have only ever previously met on the Internet, or by email or in a chat room, unless I take a trusted adult with me.
- I am aware that some websites and social networks have age restrictions and I will abide by these.
- I am aware that, at all times, my online activity should not upset or hurt other people, and that I will not put myself at risk.
- I will not take or distribute images of anyone without their permission.
- I will immediately report any damage or faults, involving equipment or software, however this may have happened.
- I will not install, or attempt to install, programmes of any type on a computer, nor will I try to alter computer settings.

When using the Internet for research or recreation, I recognise that

- I should ensure that I have permission to use the original work of others in my own work (and cite relevant references). Where work is protected by copyright, I will not try to download copies (including music and videos). When using ChatGPT or other AI-derived content I will ensure to highlight this is the case and will not try to pass the content off as my own.

- When I am using the Internet to find information, I should take care to check that the information I access is accurate as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

- I understand that I am responsible for my actions, both in and out of the Academy.

- I understand the Academy also has the right to take actions against me if I am involved in incidents of inappropriate behaviour covered in this agreement, even when I am out of the Academy, and where they involve my membership of the Academy community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy internet/intranet, detentions, suspensions, contact with parents/carers and in the event of illegal activities, involvement of the police.