E-Safety Policy

Trinity MAT

Trinity Multi-Academy Trust

Policy	**E-Safety Policy**
Date of review	**October 2022**
Date of next review	**October 2023**
Lead professional	**Director of IT**
Status	**Non-Statutory**

Purpose

Please note: this policy should be read alongside the academy's policies and procedures on Child Protection and Safeguarding.

1. The purpose of this e-Safety policy statement is to:

1.1. Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the Internet, social media or mobile devices.

1.2. Provide staff and volunteers with the overarching principles that guide our approach to online safety.

1.3. Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

Each academy within the trust has invested in a range of resources, including computers, iPads and other mobile devices, to support learning. A key part of learning is access to the Internet and all computers have internet access. By understanding and following these rules it will ensure that everyone keeps safe, and you can maximise the value you gain from your time online. This policy statement applies to all staff, volunteers, children and young people and anyone involved in the academy's activities.

If you have any questions about this e-Safety policy, please contact a member of the IT team, or speak to your tutor or class teacher, who will be able to help. You should also know that your academy

reserves the right to monitor all activities on academy resources and use of the Internet when connected through the academy network.

2. Legal Framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children - we make particular reference to Keeping Children Safe in Education (September 2022).

3. We believe that:

- Children and young people should never experience abuse of any kind.
- Children should be able to use the Internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

4. We recognise that:

- The online world provides everyone with many opportunities, however, it can also present risks and challenges.
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep children and young people safe online, whether or not they are using their academy's network and devices.
- Working in partnership with children, young people, their parents, carers and other agencies, is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

5. We will seek to keep children and young people safe by:

- Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults.
- Supporting and encouraging the young people using our service to use the Internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Supporting and encouraging parents and carers to do what they can to keep their children safe online.

- Developing an online safety policy for use with young people and their parents or carers.
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person.
- Reviewing and updating the security of our information systems regularly.
- Ensuring that usernames, logins, email accounts and passwords are used effectively.
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Providing supervision (where necessary), support and training for staff and volunteers about online safety.
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

6. If online abuse occurs, we will respond to it by:

- Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole, into account.
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.
- N.B. - See Appendix B of our Anti-Bullying policy for more information about how we respond to cyberbullying.

7. General e-Safety advice for students - protecting yourself online

7.1. Technology has revolutionised the world we live in today. Computers, the Internet and mobile telephones have made communication easier and faster. The Internet is a wonderful resource which has many benefits to your studies. You do however need to be aware, and careful, of how you use these resources. Remember, that whatever information you read online, that there is little quality assurance to check the accuracy of what you have come across.

7.2. If you follow the 4 Cs of online safety, you will be able to keep yourself safe online. See the information below:

Content

I've seen/been sent inappropriate content online. What should I do?

Make sure that you tell someone at home or at school. Call it out!

Content: Being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

I've been contacted by someone I don't know, and they've said something unpleasant/I don't like. What should I do?

Make sure that you tell someone at home or at school. Call it out!

Contact: Being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct

I've been sent a picture/video that is explicit. What should I do?

Make sure that you tell someone at home or at school. Call it out!

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce

I've got involved with/know someone who is gambling online. What should I do?

Make sure that you tell someone at home or at school. Call it out!

Commerce: Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

8. Stay SMART online:

To stay safe online, particularly when using Instant Messaging, chat rooms and social networking sites, there are some simple rules to follow, known as the SMART rules:

S - Keep safe by being careful not to give out personal information - such as your name, email, phone number, home address or academy name - to people you do not trust online.

M - Meeting someone you have been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then, only when they can be present.

A - Accepting emails, IM messages, or opening files, pictures or texts from people you do not know or trust can lead to problems - they may contain viruses or nasty messages.

R - Reliable, someone online may be lying about who they are and information you find on the Internet may not be reliable.

T - Tell your parent/carer or a trusted adult in the academy if someone or something makes you feel uncomfortable or worried. You can report online abuse to the police at www.thinkuknow.co.uk but we would prefer that you talk to us about anything that worries you.

9. Academy network - confidentiality

This section is about how you should look after your account, and our expectations of you, in relation to keeping your log-in secure.

- All students are provided with a unique log-in to access both the academy network and email, along with other linked accounts. Students should keep their password secret.

9.1. If you suspect that another student knows your password, you should change it immediately and inform a member of staff.

9.2. If you forget your log-in or password, you should contact a member of the IT team as soon as possible to have it reset.

9.3. Each student has their own secure file storage area which should only be used for storing academy work, and use of their own personal OneDrive. It is your responsibility to keep this area tidy and to delete any unwanted files.

9.4. Students should never attempt to access another student's user area.

9.5. Computers should be used for academy work only and should not be used for playing games or social networking, unless you have been given permission by a member of staff.

9.6. As with any academy property, you must not tamper or damage computer equipment in any way. This includes:

- Graffiti.
- Altering the display properties of the monitors without permission.
- Unplugging or moving devices such as keyboards and mice.
- Maliciously reconfiguring devices to alter functionality.
- Eating and drinking is strictly prohibited near computers or mobile devices.
- Students are encouraged to utilise OneDrive through Office 365 if you need to access documents away from your academy. This ensures files and data remain safe and secure. Only in specific circumstances are USB sticks/removable media allowed and your teacher will inform you where there is a specific need. Removable media must be encrypted to use on academy systems.

10. Internet and VLE usage - in your academy

This section is about using the Internet whilst at your academy. Normally any students who have access to the Internet are supervised by a member of staff. However, when working as independent learners we expect you to use the Internet in a sensible way. All computer/internet activity is remotely monitored and recorded including down to keystroke level. The academy has an internet filtering system which prevents access to inappropriate content. Students should be aware:

10.1. Any attempt to bypass the internet filtering system is strictly prohibited. Unfortunately no internet filtering system is perfect. If any inappropriate content is accidentally accessed, a member of staff should be informed immediately.

10.2. Unless you have been given permission by a member of staff, you must not access chat rooms, instant messaging or social networking sites (e.g. Facebook, Instagram, Twitter) from the academy network. You should be careful when accessing these sites in your own time and we would encourage you to make sure your parents know you have accounts for social networking sites.

10.3. Students are provided with an email address which may be used for appropriate communication within the academy or for other educational purposes. You should only use your academy email account to communicate with other students or staff.

11. Achievement and Behaviour

Using the Internet, computers or other resources is treated the same as any other academy property or resources. Where you have behaved above expectations, such as a quality piece of work, reporting concerns, or showing your awareness of e-Safety, then this will be awarded with achievement points. Equally, staff will follow the Behaviour policy and there will be consequence points if internet access is abused, or if any of the rules above are ignored. You may also have your access to the Internet or PCs limited.

12. Child on child abuse

Students should adhere to our Behaviour policy when using the Internet inside and outside of the academy. Students must not use ICT or the Internet in a way to purposefully harm others. This includes:

- Name-calling.
- Threatening language, pictures and videos.
- Bullying.
- Sending of inappropriate images.
- Sexual harassment - If you are identified as being involved in this, then the academy will apply sanctions in line with the Behaviour for Learning policy.

We encourage students and parents to report any examples of poor behaviour online to a member of staff in the academy.

13. More information on where to go for help

If you come across something online or in your academy that makes you feel uncomfortable or you feel is wrong, you should try to talk to someone. It might be your parent/carer or a trusted adult in your academy. We would encourage you to say something so we can help or put your mind at rest. There are other places you can go for help, such as:

CEOP (Child Exploitation and Online Protection Centre)

www.ceop.police.uk

You can report any online activity that feels uncomfortable to the CEOP. For example, it could be a conversation with someone online who you think is not who they say they are and asking you to do things that you really know are not acceptable or suggesting that you meet up with them.

CEOP is staffed by specialist police officers, social workers, counsellors and investigators, who are trained to deal with young people who have had bad experiences online. If you report anything to them they will take it seriously, investigate further and someone will follow up to make sure you are okay.

Think U Know

www.thinkuknow.co.uk

An excellent advice website with age specific information on all aspects of e-Safety.

ChildLine

www.childline.org.uk

You have probably already heard of ChildLine. If you feel that you are being bullied online you can talk to someone in confidence by calling ChildLine on 0800 1111.

Internet Watch Foundation

www.iwf.org.uk

Any content that you come across online which you think might be illegal, should be reported to the Internet Watch Foundation at www.iwf.org.uk.