Trinity Multi Academy Trust

| | |
|---|---|
| **Policy:** | e-Safety Policy (for students) |
| **Date or review:** | March 2020 |
| **Date of next review:** | March 2022 |
| **Lead professional:** | Director of IT |
| **Status:** | Non Statutory |

**Purpose**

Each academy within the trust has invested in a range of resources, including computers, iPads and other mobile devices, to support you in your 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.

Please ensure that you read through these rules, with your parents or carers, and that you understand them. If you have any questions please contact a member of the ICT 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.

Firstly, your safety online is most important.

**General e-Safety advice for students – protecting yourself online**

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.

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 don't 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.

**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.**
- If you suspect that another student knows your password you should change it immediately, and inform a member of staff.
- If you forget your log-in or password you should contact a member of the ICT team as soon as possible to have it reset.

- Each student has their own secure file storage area which should only be used for storing academy work. It is your responsibility to keep this area tidy and to delete any unwanted files.
- Students should never attempt to access another student's user area.
- 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.
- 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 Office365 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.

**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:

- 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.
- 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, 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.
- 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.

**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.

**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 aren't 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.