



E-safety Policy

Policy Details	
Policy prepared by:	Andrew Wakefield, Principal
Date reviewed:	September 2019
Approved by Governors	September 2019
Date of next review:	September 2020

“The IT manager” for logistical issues at The Edge Academy is currently Rajesh Patel. If Rajesh is unavailable, staff should address the Principal. “The Principal” currently refers to Andrew Wakefield.

The academy's e-safety policy operates in conjunction with other policies including those for behaviour and safeguarding.

Aim

We recognise the value of modern technology systems and welcome their development. We continually strive to enhance their appropriate use (both within academy and outside) in order to promote the educational attainment of our students. This policy is of paramount importance as our students' access to technology is currently becoming universal and increasingly more mobile.

The technologies encompassed by this policy include all computer and Internet technologies and electronic communication devices such as mobile phones and PDAs.

Any cases of a breach of the policy will be referred to the Principal.

Internet usage

The internet is used within the academy to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the academy's management information and administration systems.

We recognise the importance of the internet as an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for students who show a responsible and mature approach to its use.

Students will use the internet outside of academy and part of our responsibility is to educate them in safe use of the technology.

The breadth of issues classified within e-safety is considerable, but the three areas of risk we prioritise when talking to students are as follows:

- Content (being exposed to illegal, inappropriate or harmful material).

Common risks we address with students within content focus on exposure to inappropriate content, including online pornography and CSE/ FGM, extremism, radicalisation, sexting, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse. We also focus on lifestyle websites, for example pro-anorexia/ self-harm/ suicide sites, and so-called “hate sites”. Equally, we believe that it is important that students are taught to check the authenticity and accuracy of any online content they look at.

- Contact (being subjected to harmful online interaction with other users).

Dangers we address with students here include grooming, all forms of cyber-bullying, as well as identity theft (including so-called “frape”, the hacking of Facebook profiles etc) and password security.

- Conduct (personal online behaviour that increases the likelihood of, or causes

harm).

Within this area, students are taught about privacy issues, including disclosure of personal information, as well as digital footprint and online reputation. They are also taught about the need to consider health and well-being, where necessary limiting the amount of time spent online (internet or gaming). Equally, we believe it is important that students are educated about the dangers of sending or receiving personally intimate images, and of infringing music and film copyright laws.

The academy's e-safety policy works alongside the academy's work in ensuring that the following national frameworks are adhered to:

Keeping Children Safe in Education
Ofsted Common Inspection Framework
Working together to safeguard children
The Prevent Strategy and Channel Guidance

Use of the internet within the academy

Amongst the uses of the internet within the academy are the following:

- Access to learning wherever and whenever convenient.
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority and DFE.

Student safety on the academy internet system

- The academy Internet facility has been designed expressly for student use and includes filtering appropriate to the age of students.
- Students are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide students in on-line activities that will support learning outcomes and plan for the students' age and maturity.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Gaining access to the academy internet

- The academy maintain a current record of all system users (including staff and students) who are granted Internet access.
- All staff with access to ICT facilities must read and sign the Staff Acceptable Use Policy before using any academy ICT resource.
- All students must read and accept the 'Student ICT Acceptable use policy' before using any academy ICT resource.

Inappropriate usage of internet and loss of privilege

Any member of staff or student in breach of the agreement for usage of the Internet will have their access curtailed immediately pending investigation.

Social Networking sites

Access to Social Networking sites for students is forbidden in academy and all such sites are blocked.

Students using such sites outside of academy have a duty to use them responsibly. Any incident of slander, abuse or defamation perpetrated on a social networking site which impacts upon one of our students, shall be treated as bullying and shall be sanctioned in accordance with the academy's behaviour policy.

Academy website

- The contact details on the website are the academy address, e-mail and telephone number. Staff or student personal information is not and shall not be published.
- Currently the Headteacher has overall editorial responsibility and ensures that content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will only be used when featured on news articles sent to press.
- No photographs of students are published on the academy website without permission from the parent/carer.
- Student work can only be published with the permission of the student.

For further details, please refer to the 'Photography and images of students policy'.

Information system security

- Academy ICT systems' capacity and security are reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting personal data

Personal data is recorded, processed, transferred and made available in accordance with the updated GDPR regulations.

Assessing risks

The academy takes 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 an academy computer. The academy can accept no liability for the material accessed, or any consequences of Internet access.

Handling e-safety complaints

- Any complaint about staff misuse must be referred to the Principal
- Any complaint about student misuse must be referred to the Vice Principal

responsible for pastoral care (currently Adam Smith, Vice Principal)

- Complaints of a child protection nature must be dealt with in accordance with the academy's safeguarding procedures.

Communication of Policy

Students

- Students are informed that Internet use will be monitored through the academy's Securus software.

Staff

- All staff are issued with this policy and its importance is explained. The policy is also available on the academy website.
- Staff are made aware that internet traffic can be monitored and traced to the individual user through the academy's Securus software. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use are supervised by the Leadership Team and have clear procedures for reporting issues.

Parents

Parents' attention is drawn to the E-Safety Policy in newsletters and on the Academy website.

Social Media

The academy also sets out clear expectations below about the use of social media by stakeholders. Staff are obliged to sign this document to confirm they agree to follow the policy. This document runs in conjunction with the academy's Adult Behaviour Policy.

The Edge Academy recognises that many staff, governors, parents, carers and pupils use the internet for personal purposes and that they may participate in social networking on social media websites such as Facebook, Twitter, Youtube, etc. In addition, staff, governors, parents and carers may set up personal weblogs or "blogs" on the internet.

Whilst staff, governors, parents and carers are free to use the internet in this way, they must ensure that they do not breach the law or disclose The Edge Academy's confidential information, breach copyright, defame the school, its staff, governors, parents, carers and pupils. They must not disclose personal data or information about any individual that could breach GDPR regulations. They should keep completely confidential, any information regarding the children, their families or other staff which is learned through the school.

The purpose of this policy is to outline the responsibilities of staff, governors, parents and carers setting up personal websites and blogs and using social networking websites. This policy relates to material posted on public areas and those restricted to certain individuals.

SOCIAL MEDIA DEFINITION

Social media technologies take on many different forms including magazines, Internet forums (messageboards), weblogs (blogs), social networks (Twitter, Facebook, Instagram, etc), podcasts, photographs or pictures, video and even virtual game worlds (Moshi Monsters, Club Penguin, etc).

WEBSITES AND BLOGS

The following guidelines apply:

- Staff, governors, parents and carers must not disclose any information that is confidential to the school or any third party that has disclosed information to the school.
- Staff, governors, parents and carers should not link any personal websites, social networking sites etc to the school's website.
- Staff, governors, parents and carers must not use the school website, internet systems, e-mail addresses or intranet for their weblog and staff must not write their weblog in employer time.
- If a member of staff, governor, parent or carer is asked to contribute to an official weblog connected to the school, then special rules will apply and they will be told in detail how to operate and what to write.
 - The Edge Academy will not tolerate criticisms through social media websites and blogs. If a member of staff feels aggrieved then they must follow the procedures outlined in the Complaints and Whistleblowing Policy.

SOCIAL NETWORKING SITES

The school respects a member of staff's right to a private life. However, the school must also ensure that confidentiality and its reputation are protected. The school expects all staff, governors, parents and carers to:

- Ensure that they do not conduct themselves in a way that is detrimental to the school.
- Take care not to allow their interaction on these websites to damage working relationships between members of staff and clients of the school.

IMPORTANT CONSIDERATIONS

When writing a weblog and placing information on social networking sites, staff, governors, parents and carers should follow these guidelines:

- Do not include any information that breaches copyright and should link to other material rather than cutting and pasting it
- Do not defame (libel) anyone. A member of staff, governor, parent or carer who makes a defamatory statement that is published on the internet may be legally liable for any damage to the reputation of the individual concerned
- Do not include personal information about an individual without his/her consent, otherwise they risk breaching GDPR regulations, which is a criminal offence

- Do not include material that is abusive, defamatory, sexist, racist or that could be interpreted as harassment or bullying
- Do not bring The Edge Academy into disrepute
- Staff should only access social media sites in their own time
- Staff should not comment on any posts made by others relating to the school
- Staff should not share or discuss matters relating to the school
- It is not advisable to invite parents/carers to become your friends on social networking sites. There may be a conflict of interest and security and privacy issues, but where relationships are already established, staff should proceed with caution, being fully aware of the social media guidelines and the teacher's code of conduct
- Staff should not accept friend requests from The Edge Academy pupils under any circumstances
- Staff should use the privacy settings available (see Adult Behaviour Policy)
- Staff should not share personal conversations.
- Staff should behave respectfully and should not engage in topics that may be considered objectionable or inflammatory.

CYBER BULLYING

The Edge Academy is committed to ensuring that all of its staff, parents/carers and pupils are treated with dignity and respect. Bullying and harassment of any kind will not be tolerated. Cyber-bullying methods could include text messages, emails, phone calls, instant messenger services, circulating photos or video clips or by posting comments on web sites, blogs or in chat rooms. Personal blogs that refer to colleagues without their consent is also unacceptable. Staff, governors, parents and carers who cyber-bully could also face criminal prosecution under various laws, including the Malicious Communications Act 1988.

PERSONAL USE OF THE INTERNET

The Edge Academy does not allow personal use of the internet during session times and there is also clear guidance in the Adult Behaviour Policy regarding internet use generally.

DISCIPLINARY ACTION

If necessary, action will be taken against any member of staff, governor, parent or carer who is found to have breached this Policy. Staff should also refer to the Disciplinary Policy.

SECURITY AND IDENTITY THEFT

Staff, governors, parents and carers should be aware that social networking websites are a public forum, particularly if they are part of a 'network'. Staff, governors, parents

and carers should not assume that their entries on any website will remain private. Staff, governors, parents and carers must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and, for example, favourite football team which can form the basis of security questions and passwords.

I sign to accept and be bound by these terms:

Signature:

Name (printed):

Date:

