



**PADGATE
ACADEMY**

e-Safety Policy

Date approved by the Governing Body	13 February 2019
Signature of Chair of Padgate Academy Governing Body	Mr G.A. Wilson
Signature of Academy Principal	Mrs M. Barclay
Next review	September 2021

Contents

Contents

Introduction and General Principles	3
Thorough eSafety.....	3
Teaching and Learning	3
Why Internet Use is Important	3
Internet Use will Enhance Learning	3
Students will be Taught to Evaluate Internet Content	3
Managing Internet Access.....	4
Information System Security.....	4
eMail	4
Published Content and Academy Websites	4
Publishing Students Images and Work	4
Social Networking and Personal Publishing.....	5
Managing Filtering	5
Managing Video Conferencing.....	5
Managing Emerging Technologies	5
Protecting Personal Data	5
Authorisation	6
Assessing Risks	6
Handling eSafety Complaints	6
Communication of Policy	6
Students	6
Staff, Trustees and SOAC Members.....	6
Parents	7
Monitoring, Evaluation and Review.....	7

Introduction and General Principles

Padgate Academy believe that the use of information and communication technologies brings great benefits. The Academy recognises the e-Safety issues and this policy will ensure appropriate, effective and safe use of electronic communications.

The e-Safety policy encompasses internet technologies and electronic communications such as mobile phones and wireless technology. The Academy e-Safety policy will operate in conjunction with other policies including those for Student Behaviour, Anti-Bullying, Curriculum, ICT Acceptable Use, Safeguarding, Social Media and Data Protection.

Thorough eSafety

eSafety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-Safety policy in both administration and curriculum, including secure academy network design and use.
- Safe and secure broadband.
- National Education Network standards and specifications.

Teaching and Learning

Why Internet Use is Important

The internet is an essential element in 21st century life for education, business and social interaction. The Academy has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

Internet Use will Enhance Learning

The Academy internet access will be designed expressly for student use and will include filtering appropriate to the age of students.

Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be Taught to Evaluate Internet Content

The Academy will ensure that the use of internet derived materials by staff and by students complies with copyright law.

Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information System Security

- Academy ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly

eMail

Students may only use approved e-mail accounts on the Academy system. Students must immediately tell a teacher if they receive offensive e-mail.

Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on academy headed paper.

The forwarding of chain letters is not permitted.

Published Content and Academy Websites

The contact details on Academy web sites will be academy addresses, e-mails and telephone numbers. Staff or students personal information will not be published.

The Principal (or nominee) will take overall editorial responsibility and ensure that content is accurate and appropriate in each academy.

Publishing Students Images and Work

Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.

Students full names will not be used anywhere on any Academy web site or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of students are published on any Academy web site.

Work will only be published with the permission of the student and parents.

Social Networking and Personal Publishing

The Academy will block/filter access to social networking sites. Newsgroups will be blocked unless a specific use is approved.

Students will be advised never to give out personal details of any kind which may identify them or their location.

Students must not place personal photos on any social network space.

Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and know how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others.

Managing Filtering

The Academy will work in partnership with the Internet Service Provider to ensure systems to protect students are reviewed and improved.

If staff or students discover an unsuitable site, it must be reported to the e-Safety Co-ordinator or the Network Manager in their academy.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Video Conferencing

Video conferencing should use the educational broadband network to ensure quality of service and security rather than the internet.

Students must ask permission from the supervising teacher before making or answering a videoconference call.

Video conferencing will be appropriately supervised for the students age group.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use is allowed in any academy.

Mobile 'phones will not be used during lessons or formal academy time. The sending of abusive or inappropriate text messages is forbidden.

Staff will be issued with an academy phone where contact with students is required.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Padgate Academy Data Protection Policy.

Authorisation

All staff must read and sign the 'ICT Acceptable Use' form before using any academy ICT resource.

Each academy will maintain a current record of all staff and students who are granted access to academy ICT systems.

Students must apply for internet access individually by agreeing to comply with the ICT Acceptable Use statement.

Parents will be asked to sign and return a consent form.

Assessing Risks

The Academy will take 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 a Academy computer. The Academy cannot accept liability for the material accessed, or any consequences of internet access.

The Academy will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.

Handling eSafety Complaints

Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Principal.

Complaints of a child protection nature must be dealt with in accordance with Academy Safeguarding Policy.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Students

e-Safety rules will be posted in all networked rooms. Students will be informed that network and internet use will be monitored.

Staff, Trustees and SOAC Members

All staff will be given the Academies e-Safety Policy and its importance explained.

Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Parents

Parents' attention will be drawn to the Academy e-Safety Policy in newsletters, the academy prospectus and on the academy web site.

Monitoring, Evaluation and Review

The Board will review this policy at least every two years and assess its implementation and effectiveness.