Tolworth Girls' School & Sixth Form

e-SAFETY POLICY

Governing Body Committee: Finance, Assets & Audit (F, A & A)
Date approved: March 2023 (F, A & A 13/03/23)
Next review: March 2025

This policy should be read in conjunction with the:

- Anti-bullying
- Keeping Children Safe in Education (safeguarding)
- ICT Acceptable Usage Policy
- Student Behaviour Policy
- Data Protection Policy
- Disciplinary Procedure

Introduction

Information, Communication Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults.

ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Pod casting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

The Governing Body of Tolworth Girls' School & Sixth Form is committed to providing a safe and healthy workplace for all employees and to ensure that their work does not adversely affect the e-safety of other people.

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

With the Headteacher and her staff, the Governing Body acknowledges they have a duty of care to provide a safe and healthy e-environment for all students.

Scope

This policy and procedure applies to: -

- All Governors, staff and students
- Any third party people as part of academy activity

Responsibilities

a) The **Governing Body** is responsible to:

- Set the e-Safety policy
- Appoint one governor to have oversight of e-safety matters
- Review this e-Safety policy either every year or in response to any major incident

b) The **Headteacher or her designate** is responsible to:

- Day to day responsibility for all e-safety matters in the academy
- Liaise with Governors as appropriate on e-Safety policy issues
- Ensure that e-safety procedures are implemented
- Ensure the ICT Acceptable Usage policy is signed by all staff and students
- Arrange for staff e-safety training as appropriate

Parents/ Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. The academy will therefore take every opportunity to help parents/carers understand these issues through parents/carers' evenings, newsletters, website / VLE and information about national / local e-Safety campaigns / literature. Parents/carers will be responsible for:

• endorsing (by signature) the ICT Acceptable Usage Policy

• accessing the school website / VLE / on-line student / student records in accordance with the relevant academy ICT Acceptable Usage Policy

Students

- are responsible for using the academy ICT systems in accordance with the ICT Acceptable Usage Policy, which they will be expected to sign before being given access to school systems.

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- will be expected to know and understand academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand academy policies on the taking / use of images and on cyber-bullying.

- should understand the importance of adopting good e-Safety practice when using digital technologies out of school.

End to End e-Safety

e-Safety 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 from LGfL (London Grid for Learning) including the effective management of Web filtering.

Academy e-Safety Policy

Teaching and Learning

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 skill of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

- The academy should 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.

5.2 Managing Internet Access

Information system security

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

E-mail

- 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 where appropriate authorised before sending, in the same way as a letter written on academy headed paper.
- The forwarding of chain letters is not permitted.
- If issues are sensitive staff should always seek advice prior to sending email.
- Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels. For more information please see here

Published content and the academy website

- The contact details on the website should be the academy address, e-mail and telephone number. Staff or student's personal information will not be published.
- Business contact for staff will be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing student's images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified by name. Students' full names will not be used anywhere on the website or Blog, particularly in association with photographs.

- Written permission from parents/carers will be obtained before photographs of students are published on the academy website.

- Work can only be published with the permission of the student and parents/carers

Social networking and personal publishing in academy

- 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 should be advised on security and must set passwords and deny access to others. They must also be advised on how to block unwanted communications.

- Students should be encouraged to invite known friends only and deny access to others.

Social networking and personal publishing for external use

- As the social network space is public domain, students/staff must not post any information and comments that are derogatory to the academy community.

Sexting

- The sending of nude / semi naked pictures and videos is illegal. Students are made aware of the consequences of this and how to stay safe when using mobile devices and the internet. Sexting is dealt with in accordance with the Keeping Children Safe in Education (Safeguarding) policy.

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 Network Manager.

Managing videoconferencing, including use of webcam

- IP videoconferencing should use the educational broadband network where possible to ensure quality of service and security rather than the Internet.

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

- Videoconferencing will be appropriately supervised for the students' age.

Managing emerging technologies

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

- The sending of abusive or inappropriate text and any social messaging is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Act 2021.

- Should any future communication with Parents/Carers be by email, there will be protection of data.

- All data will be removed from redundant hard drives before their disposal.

Authorising and controlling Internet access

- All staff must read and sign the 'TGS ICT Acceptable Usage Policy' before using any academy ICT resource.

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

- Students and their parents/carers must read and sign the 'TGS ICT Acceptable Usage Policy'. This is sent to them via an electronic form to them prior to the students coming to school.

- 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 an academy computer. The academy cannot accept liability for the material accessed, or any consequences of Internet access

- The academy should audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate.

Handling e-safety complaints

- Complaints of Internet misuse by students will be dealt with by a senior member of staff.

- Any complaint about staff misuse will be dealt with through the staff disciplinary policy.

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

Complaints procedure

- Parents/carers will be informed of the complaints procedure.
- Concerns about any aspects of the use of internet should be addressed directly to the Headteacher.
- Staff should be cautious and use their professional judgement when using mobile phones.

Communicating the e-Policy

- Students will be informed that network and Internet use will be monitored.

Staff and the e-Safety Policy

- All staff will be given the academy 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 the Resource Director and have clear procedures for reporting issues.
- The following legislation - enforceable against public sector employees including school staff - must be considered when using the internet or email:
    - Human Rights Act 1998
    - Regulation of Investigatory Powers Act 2000 (RIPA)3
    - Data Protection Act 1998
    - Freedom of Information Act 2000
    - Copyright, Designs and Patents Act 1988, amended by the Copyright and Related Rights Regulations 2003
    - Computer Misuse Act 1990, amended by the Police and Justice Act 2006
    - Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988
- 6.13 These Acts are concerned with material that might be:
    - Criminal
    - Cause harm to young people or
    - Be otherwise unlawful

This policy will be reviewed every 2 years.

The F, A & A committee is responsible for approving this policy.