TOLWORTH GIRLS' SCHOOL & SIXTH FORM
STAFF ICT ACCEPTABLE USAGE POLICY

Reviewed and approved by the F, A & A committee: October 2018

Next Review: October 2020

INTRODUCTION

The Governors of Tolworth Girls' School & Sixth Form, the Headteacher and staff wish to encourage students to use the ICT facilities at school for educational purposes. The responsible use of these facilities contributes significantly to the rich academic and personal experience of the students.

The guiding principle that underpins this policy is that ICT should be used responsibly at all times. This applies to all members of the school community.

This acceptable use policy has been created to:

- Ensure that all users have reasonable access to the ICT facilities and encourage the responsible use of all its ICT resources.
- Maintain the image and reputation of Tolworth Girls' School & Sixth Form as a responsible provider of education.
- Protect the security, reliability and privacy of Tolworth Girls' School & Sixth Form systems and network.

The following rules should be observed to ensure a secure environment in which all members of our community can study and work.

USE OF TECHNOLOGY

Technology that can be used to store, transmit or manipulate data, such as laptops/tablets, mobile devices, MP3/4 players, Personal Digital Assistants (PDAs) and USB media, should be used responsibly and in accordance with other school policies, rules and codes of conduct.

ACCOUNT SECURITY

Users are responsible for the protection of their own network account and their email account. They should not divulge **any** of these passwords to **anyone.** ** If a user suspects their password has been discovered by another person it must be changed immediately.

Users should not log on to or use any account other than their own ** and should either lock the workstation or logoff when leaving, even for just a short period of time. It is the responsibility of the user to ensure that the data in his/her account(s) is protected.

USE OF FACILITIES

It is not acceptable to: -

- Attempt to download, store or install software on any school IT equipment **.
- Attempt to introduce a virus or malicious code to the network.
- Attempt to bypass network or system security.
- Attempt to access another user's account. **
- Attempt to gain access to an unauthorised area or system.
- Attempt to use any form of hacking/cracking software or system.
- Connect any device to the network that acts as a Wireless Access Point (WAP) or router.
- Connect any device to the network that has access to the Internet via a connection not provided by the school.
- Access, download, create, store or transmit material that is indecent or obscene, material that could cause annoyance, offence or anxiety to other users, or material that infringes copyright or is unlawful.
- Engage in activities that waste technical support time and resources.

INTERNET ACCESS

The school's Internet service is filtered to prevent access to inappropriate content and to maintain the integrity of the computer systems. Users should be aware that the school logs all Internet use.

The use of public chat facilities is not permitted. **

Users should not copy and use material from the Internet to gain unfair advantage in their studies, for example in controlled assessments. Such actions may lead to disqualification by examination boards.

Users should ensure that they are not breaking copyright restrictions when copying and using material from the Internet.

EMAIL

Students are not allowed to use email during lessons, unless the teacher has specifically permitted its use.

If a user receives an email from an unknown person, or one that is offensive or upsetting, the relevant Head of Year or a member of the IT department should be contacted. Do not delete the email in question until the matter has been investigated.

- Sending or forwarding chain emails is not acceptable.
- Sending or forwarding emails to a large number of recipients is acceptable but only for a good reason. Before doing so, the user must obtain permission from the Resource Director or the Network Manager.
- Do not open attachments from senders you do not recognize, or who look suspicious.
- Users should regularly delete unwanted sent and received emails.
- Students may only use the email facilities provided by TGS when in school.

INSTANT MESSAGING

- Students are not allowed to use IM facilities during lessons, unless the teacher for that lesson has permitted its use.
- If a user receives a message from an unknown person, or which is offensive or upsetting, the relevant Head of Year or a member of the IT Department should be contacted. Copy and save the message as evidence.
- Only communicate with people you know.
- Do not accept requests to join your contact list from people you do not already know.
- Never accept a file or a download from people you do not know, or that looks suspicious.
- Do not use a screen-name that is offensive, or gives away additional personal information.
- Do not add unnecessary personal information to your IM profile or account details.
- Do not add or allow your profile, screen-name or contact information to be shown in online public directories.

PRIVACY AND PERSONAL PROTECTION

- Users must, at all times, respect the privacy of other users.
- Users should not forward private data without permission from the author.
- Users should not supply personal information about themselves or others via the web, email or other electrical/digital means. **
- Users must not attempt to arrange meetings with anyone met via the web, email or other electrical/digital means. **
- Users should understand that the school reserves the right to access all electronic information held on the School IT systems of students and staff. We may also be required to act on behalf of official bodies The school has Impero software, which scans all computer usage for inappropriate use, matters of concern will be investigated by Student Support workers. The Headteacher or Resource Director will investigate concerns involving staff.

Students should report any unsafe or malfunctioning equipment to their class teacher in the first instance and subsequently to a member of the IT support department.

DISCIPLINARY PROCEDURES

Those who misuse the computer facilities and do not adhere to any sections of this policy will be subject to normal school disciplinary procedures, as well as having their access to ICT facilities withdrawn. In the case of persistent or serious breaches of the policy legal action may be taken under the terms of the Computer Misuse Act or other relevant legislation.

SUPPORT

If you have any questions, comments or requests with regards to these matters, please do not hesitate to contact the Director of Resources or a member of the Senior Leadership Team member via the school office.

******In order to carry out **essential** aspects of their professional role within school, staff in **specific and unusual** circumstances and with the consent of their line manager may have to act differently to the stated practice. Staff will be assumed to be acting in good faith at all times and to safe guard themselves and the school, these instances should be recorded in writing.