THE ROYAL BALLET SCHOOL

POLICY ON THE ACCEPTABLE USE OF ICT: UPPER SCHOOL STUDENTS

Introduction

The Royal Ballet School aims to ensure secure and supervised access to ICT for all students, at the School, Jebsen and Wolf Houses and the Long Acre flats. This policy is intended to support this aim by outlining acceptable uses of ICT for students while they are in the care of the School. It applies to the use of The Royal Ballet School network and any computer equipment connected to it, internet and electronic mail facilities, file-servers, messaging services, and any networks or hardware, including but not limited to that provided by the School. It applies to any personal devices including computers, tablets, mobile phones, MP3 players, cameras, games players and any other equipment that can be used to access, store or record data or media files.

Access to the computer network is a considerable privilege and it is the students' responsibility to restrict themselves to usage which is ethical and appropriate. Failure to comply with the rules which govern the use of the network may lead to punishment of the student. In serious cases, parents will be informed. Further action will be carried out if deemed necessary.

Practice

Every student is issued with a School ICT account and password. Students must not interfere with the work of others or the system itself.

Students must not:

a) create, store, transmit or cause to be transmitted material which is offensive, obscene, indecent or defamatory or which infringes the copyright of another person
b) use another person's password or account
c) transmit any messages or prepare files that appear to originate from anyone other than themselves
d) gain or attempt to gain unauthorised access to other people's files or facilities or services accessible via local or national networks or transmit any confidential information about the School
e) gain or attempt to gain access to inappropriate sites
f) attempt to get around service limitations placed on network use by the School (or its agents)
g) send any message internally or externally which is bullying, abusive, humiliating, hostile or intimidating.

They must compose any e-mail (or other electronic communication) with courtesy and consideration.

Security

Students must protect all devices and accounts with passwords. not disclose passwords to anyone and must not attempt to discover or use the passwords of others. They must take sensible precautions to avoid Internet viruses.

Confidentiality

Any School information or records including details of students, parents and employees whether actual, potential or past, other than those contained in authorised and publicly available documents, must be kept confidential unless the School's prior written consent has been obtained. This requirement exists both during and after a pupil's time at the School. In particular, students or ex-students must not use such information for the benefit of any future employer.

Monitoring

The School reserves the right to monitor communications and general network usage in order to:

a) Protect students
b) Establish the existence of facts
c) Prevent or detect crime
d) Investigate or detect unauthorised, suspicious or inappropriate use of the
e) School's ICT systems
f) Ensure the effective operation of the School network and its systems.

Random checks

The School reserves the right to perform random checks on laptops and other electronic devices for illicit activities or material.

Sanctions

In the event of any breach of the policy, appropriate sanctions are imposed in line with the School's behaviour and exclusions policy: this may include the restriction of a pupil's access to the School network, the confiscation of any personal or shared devices being used to infringe these or any wider School rules, or more serious sanctions including temporary or permanent exclusion. If the breach is of a criminal nature, the Police and Local Safeguarding Children's Board (LSCB) may be involved. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The Child Protection Co-ordinator handles all such situations.

Confiscation

As part of the School's Child Protection responsibilities it may be necessary to confiscate from any student while at the School his or her computer, mobile telephone, MP3 player or any other device capable of digital recording. The confiscated items are inspected and returned as rapidly as reasonably practicable. If the items contain inappropriate material, that material is wiped from the item's memory.

Education

The School recognises that blocking and barring sites is no longer adequate. It aims to teach all students to understand why they need to behave responsibly if they are to protect themselves.

Working with parents

The School seeks to work closely with parents and guardians in promoting a culture of e- safety. The School always contact parents if there are worries about a pupil's behaviour and encourages parents to share concerns with the School.

Cyber bullying

The School's preventative measures and procedures for dealing with cyber bullying are found in the Anti-Bullying Policy.

Mobile Phones

The School does not normally expect staff and students to communicate with each other by text or mobile phones. The Academic and Pastoral Head gives permission to the School secretary and the Accommodation and Pastoral Managers to call or text students' mobile 'phones to ensure the students' health and safety. The Educational Visits Policy explains the circumstances when other staff may be permitted to call or text students: students' mobile numbers are deleted at the end of the visit.

Cameras

The use of cameras, including those on mobile phones, is not permitted at any event or in any place connected with the School where they could justifiably be regarded as an interference or intrusion. Any photographs taken must be for use as a memento and should never involve situations that others could regard as harassing or embarrassing. No photographs may be published on the internet, and great care should be taken over sending or forwarding photographs on and from mobile phones. Especial care must be taken in the Houses and flats, especially in students' bedrooms, to avoid embarrassment or harassment. Photographs may never be taken in bathrooms or changing rooms.

Safe use of personal electronic equipment

No one should put anything onto the web that they would not be prepared for parents, teachers or future employers to read or see. The web is completely public and it is very hard to remove anything from it. Any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later. Once images are forwarded to others, the same applies.

More information

A number of organisations offer web safety guidance. Two especially helpful ones are:

a) The Child Protection and Online Exploitation Centre (CEOPS), whose website ceop.police.uk contains a link to www.thinkuknow.co.uk.
b) Childline: www.childline.org.uk/SafeSurfing.