ROYAL BALLET SCHOOL

SETTING THE STANDARD

STUDENT ICT ACCEPTABLE USE POLICY

SEPTEMBER 2026

This policy is an extension of the Student Code of Conduct, covering specifically the use of 'The Royal Ballet School networks', any computer equipment provided by the School and/or any mobile device connected to the network or used to access the internet whether personal or provided by School. This policy is also intended to raise student awareness of the risks of the online environment and encourage a safe approach to this and social media in the broader sense.

Students will be asked to sign to indicate their understanding and acceptance of this Policy on the annual Student Induction checklist.

Risks of the online environment

Students should be aware that the online environment can pose a significant risk to them and to their peers. These risks include child-on-child abuse and cyber-bullying (including sexting), the possible befriending of young people by adults (sometimes posing as young people) for sexual activity, the encouraging of young people to get involved in radical, extremist or racist behaviour as well as exposure to illegal or inappropriate material such as pornography, violent computer games and so on. Other areas of online content may also pose a risk to young people such as sites that promote inappropriate ideas around disordered eating, self-harm and so on.

It is often much easier for young people to do things online that they would never consider doing in a face to face environment. This can mean that students are tempted to do things that are unkind, that break school rules, that are even illegal and can, therefore, get them into serious trouble both in School and even with the Police.

All students need to be aware of these risks when using the School network (which is monitored and checked regularly) and when using 3G/4G/5G on personal mobile devices. The School rules and the law apply whether or not you are using a personal device or a School computer to access inappropriate material or behave in a manner that is not in line with either the School rules or the law.

If you have any concerns or worries about these risks, please speak to a member of staff or one of the people or organisations listed on the 'Worried About' notices. There is no problem too big or too small that it cannot be sorted out.

Harassment

Harassment and bullying may be defined as any form of unwelcome behaviour that affects a person's dignity. It's the conduct of one person against another, or others, when an intimidating, hostile or offensive atmosphere is created for the complainant(s). Harassment is defined as per the Equity Act 2010 as being:

"…unwanted conduct related to a relevant protected characteristic, which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that individual."

Harassment may be a single act or persistent behaviours and will amount to unlawful discrimination if it relates to one of the nine protected characteristics under the Equality Act:

- Age
- Disability
- Gender Reassignment
- Ethnicity
- Religion/Belief
- Sex
- Sexual Orientation
- Pregnancy/Maternity
- Marriage/Civil Partnership

The School also finds harassment relating to caring responsibilities, gender identity and working status, (i.e. working part-time), unacceptable. The Protection from Harassment Act 1997 also makes harassment potentially a criminal offence and gives the harassed party the right to legal redress.

COMPUTER FACILITIES

1. Overview

At The Royal Ballet School we allow all students access to the School computer network, enabling them to use standard applications (word processing, spreadsheet, database etc.) as well as online facilities such as the Internet and email.

On arrival at the school each student is issued with a username, password and an e-mail address. Students will also receive the student Wi-Fi code to enable them to access the school network.

Access to the computer network is a privilege and it is the student's responsibility to restrict themselves to usage which is within these guidelines, legal, ethical and appropriate.

Failure to comply with the rules which govern the use of the network may result in either:

(a) Sanction of the student, for example by means of the detention systems which operate at different levels in the school.
(b) The students use of the School system being suspended
(c) In serious cases students may be subject to more serious sanctions under the Behaviour Policy, such as suspension. Parents may also be informed when serious breaches of the Acceptable Use of ICT Policy have occurred.

Students are required to check their School emails daily and make use of technology in support of their studies in all subjects, including the writing up of coursework assignments and other projects.

Recreational use of the network is also permitted but students should only use the student external network which is accessed through the student Wi-Fi for their personal devices. Recreational use of the school Wi-Fi is limited to between 07.00 and 22.00. Students should not attempt to access the Internet for personal use outside these times. At White Lodge, students in Years 7- 9 are required to hand in ALL of their personal devices at bedtime.

The Royal Ballet School provides a network environment in which students can assume that their legitimate use of computers and the data that they store, are secure against interference by other users. Students should not, however, assume that their activities are completely private.

The School now monitors user accounts, fileserver space and the use of the internet at all times. This means that records of usage, files that have been stored, and e-mail messages that have been sent or received or websites that have been visited are all monitored automatically and the accessing of material that may pose a risk to a student will then be flagged up by the system. The School does not wish to intrude on a student's privacy, but does wish to keep students safe.

2. Rules

The following rules apply in all the areas of The Royal Ballet School where computers, laptops and other equipment are provided for access by students.

Use of School ICT equipment

Students must:

- Obtain permission from staff before using the school laptops, iPads and other equipment.

- Use the primary or secondary laptop assigned to them. This laptop must be returned and plugged into the laptop trolley immediately after use.

- Behave in an orderly and sensible manner when using School ICT equipment.

- Not consume food or drink of any kind whilst using School ICT equipment.

- Report (without delay) damage to laptops or other equipment to a member of staff. The same applies to any apparent malfunction of equipment.

3. Use of the Network

a) When logging on to the network, a student must only use his or her own user identification and password. Any attempt to impersonate another user will be treated as a serious offence, as will any attempt to interfere with data stored on the network by another user. These activities are in fact illegal under UK law.
b) Never, under any circumstances, use another person's account or attempt to log on as a System Administrator.
c) Never use proxy sites (anonymous surfing sites,) VPNs to bypass the school filtering systems and access contents that are blocked by The Royal Ballet School.
d) Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user. The Royal Ballet School network or other networks connected to the Internet must not be vandalised. This includes the uploading or creating of computer viruses.
e) Harassment is defined as the persistent annoyance of another user, or interference with another user's work. Harassment must never occur; this includes, but is not limited to, the sending of unwanted email (see below).
f) If a security problem on The Royal Ballet School system is identified, a student must notify a member of staff immediately. They must not demonstrate the problem to other users.
g) Students must never divulge their passwords to other students or to users of computers outside The Royal Ballet School. Any student who suspects that this has happened accidentally should change their password without delay and advise a member of staff.
h) Before leaving a computer, students must always log off the network and check that the logging out procedure is complete. If the computer is to be left temporarily it should be locked to ensure that it remains secure.
i) Students must not attempt to gain access to the local drive of any machine or to create local accounts (administrative or otherwise).
j) It is strictly forbidden to attempt to share drives, folders or files across the network.
k) Only software that has been provided on the network may be run on the computers. Students are not permitted to import or download applications or games. In many cases it is illegal to do so.

l) It is a breach of The Royal Ballet School's policy on plagiarism (and of the rules of examination boards) to pass off another's work as your own. This prohibition extends to information accessed electronically as it does to that gained in other ways.
m) Students must be aware of, and comply with, the restrictions placed on certain kinds of usage; notably the playing of games on equipment and at particular times of the day, where others wish to do academic work.
n) Students may not physically attach any personal ICT equipment into the School network. They may however use the student external network which is accessed through the student Wi-Fi for their personal equipment.
o) Students should never download films, games or other items illegally through the School system.
p) The School Virtual Learning Platform, (MSTeams), is managed by the School. Students in Years 7-11 inclusive are prohibited from using the 'chat' function to communicate with other students unless a member of staff is in the chat or chat group. Chatting to teachers is acceptable to ensure timely support and guidance

4. Internet and Email

The School's filter system is continually updated, though there can be no absolute guarantee that unsuitable material is not available to users. If you encounter any material that you believe is not suitable, please let staff know as soon as possible.

Rules

Email and the internet represent an important learning resource; however, they can be wasted or abused. When using these facilities, students are expected to use their common sense and behave with normal standards of courtesy. Students should not access, download or share age-inappropriate material such as games or other material such as films that are certified for older age groups.

A. General Netiquette

Students must **NOT** (when using School or personal equipment):

a) Send electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable. It is essential that students are mindful that such behaviour could be seen as cyberbullying - *see Anti-Bullying Policy and Behaviour Policy.*
b) Create, store, transmit or cause to be transmitted material which is offensive, obscene, indecent or defamatory or which infringes the copyright of another person.
c) Disclose to a third party the personal details of any other student.
d) Access any inappropriate internet site e.g. adult sites, gambling sites or dating sites. This list is illustrative rather than exhaustive.
e) Take photos/video or other digital recordings of staff or their peers without their specific permission. This includes the use of camera enabled smart devices (such as Meta Ray-Ban glasses.
f)

g) Upload or download any unauthorised software or attempt to run that software. In particular hacking, encryption and other system tools are expressly forbidden.
h) Use the computer network to gain unauthorised access to any other computer network.
i) Engage in activities that are prohibited under UK Law. Thus, the transmission of material subject to copyright or protected by trade secret is forbidden, as of course is any threatening or obscene matter

This list is illustrative rather than exhaustive.

B. Personal Safety

In addition, students need to be aware that the thoughtless use of the online environment may jeopardise their personal safety either at school or outside school.

Students should therefore:

a) Never disclose the details of the school Wi-Fi codes to outside users.

b) Never arrange a meeting in person with anyone they have "met" or only communicated with by computer, without prior parental approval.

c) Not respond to messages or bulletin board items that are indecent, suggestive, belligerent, discriminatory, threatening, or which make the student feel uncomfortable or unsafe in any way. If such a message is encountered the student should inform a member of staff or their parents.

d) Be aware that any person they "meet" or communicate with online may pretend to be someone else.

e) Remember that anything they read online may not be accurate.

f) Ignore offers that involve either financial transactions or personal meetings.

g) Not disclose any personal details, such as their home address or telephone number, across social media.

h) Be aware that the Internet may be used as a medium through which extreme views and radicalisation may be promoted. Where concerns of this nature occur students should inform a member of staff or their parents.

C. Social Media

Please refer to the Student use of Social media policy

D. Good practice guidelines for the use of social media

- Think before you post.
- Do not disclose personal details such as phone numbers, email addresses or home addresses.
- Consider that what you write may well be read by a wide audience and that it may remain in the public domain for many years.
- Do not discuss school matters which could affect your reputation, the reputation of other students or staff, or the reputation of the school.
- If you notice any negative or harmful comments on social media about students, staff or the school, report it to a member of staff.
- Make sure to get permission from the Artistic Director before using the School's name in social media.

5. The use of Artificial Intelligence (AI)

Artificial Intelligence tools are now widely available and can support learning when used appropriately. The following guidance should be followed by all students

- Only use AI tools when permitted by staff
- Do not submit AI generated work as your own unless directed by a member of staff
- Check information generated by AI as it may be inaccurate, misleading and biased
- Follow staff guidance regarding the use of AI in classwork, prep and assessments

Students should not

- Use AI to cheat or plagiarise
- Upload personal information about themselves, other students, staff or families into AI systems.
- Use AI to create harmful, offensive, threatening or inappropriate content.
- Use AI to impersonate another person.

Deepfakes, AI-Generated Images and Impersonation

The school recognises that AI technology can be used to create realistic but false images, videos and audio recordings.

Students should not

- Create, possess or share deep-fake images of any student, staff member or other person.
- Create AI-generated nude, semi-nude or sexualised images.
- Use AI tools to alter images of another person without their consent.
- Use AI to imitate another person's voice, appearance or identity
- Share manipulated content intended to embarrass, bully, threaten or humiliate

Cyberbullying

- The school has a zero-tolerance approach to cyberbullying.
- Cyberbullying may include:
- Sending abusive messages.
- Sharing rumours online.
- Creating fake profiles.
- Posting embarrassing photographs or videos.
- Excluding others from online groups.
- Sharing private information without permission.
- Using AI-generated content to harass, threaten or humiliate another person.

Respect, Equality and Inclusion

The school is committed to creating a culture of respect and inclusion.

Students must not use technology to:

- Share sexist, racist, homophobic, biphobic, transphobic, ableist or discriminatory content.
- Promote hatred towards individuals or groups.
- Share misogynistic or abusive content.
- Engage with online behaviour that normalises harassment or abuse.

Harmful Online Influences

Students should be aware that some online content may promote harmful attitudes or behaviours.

Students are expected to:

- critically about information encountered online.
- Discuss concerns with a trusted adult.
- Report content that promotes hatred, abuse, exploitation or harmful behaviour.

The school may take action where online activity contributes to bullying, harassment, radicalisation, discrimination or other safeguarding concerns.

Misinformation and Disinformation

Students should understand that content found online is not always accurate.

Students should:

- Check information using reliable sources.
- Be cautious when sharing information online.

- Avoid spreading misinformation, fake news or conspiracy theories.

Deliberately creating or sharing false information intended to cause harm to others may be treated as a disciplinary matter.

6. Personal Devices (The school follows the guidance from the Secretary of State sent to all schools in February 2026. https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools)

Students at White Lodge and Upper School may not use mobile phones or similar devices in any academic lessons, while walking around the school buildings, or in any private areas, such as changing rooms or toilets. Students may use devices for taking video footage as part of the learning progress, if given permission to do so by a member of the Artistic Team or their teacher in GCSE Dance Studies.

Whie Lodge arrangements:

At White Lodge, all students are supplied with a school iPad.

Boarders: All phones/devices are to be left in the boarding house during the school day (08:10 am to 6:00 pm Mon-Fri, and 09:00 am to 1:00 pm on Saturday). Phones cannot be used during prep time. International students may ask for permission to use their phone to contact their parents/guardians at break time or lunchtime to take into account different time zones. Calls will be made from the house office. Phones in the houses are stored securely. Boarders may request their phones from whenever they finish their last class of the day and are back in the boarding house, which, depending on the weekly timetable, may be before 6:00 pm on weekdays and/or 1:00 pm on Saturday.

Day students: All phones/devices must be placed into a lockable pouch on arrival at school. FoH will check that the case is locked before the student accesses the school site. The student will carry the pouch with them during the day. On leaving the site at the end of the day, they can unlock the pouch using the unlock mechanism which will be situated at FoH. They will leave the pouch in the box provided so that it can be used the next day

Pupils who need their phone to monitor specific diagnosed health or SEND needs are exempt and may carry their phone at all times for this purpose only; which may include contacting their parents/guardians at any time.

Upper School arrangements:

Upper School students may use their mobile devices during the warm-up for artistic lessons but these must be turned off for the duration of the lesson unless they have been otherwise asked to do so by a member of Artistic Team.

Upper School students may use their phones in common rooms and studios (see above) but not in any other areas of the building (e.g. corridors) during the school day (08:00 am to 6:00 pm).

House Staff will request student mobile numbers at the start of the year and these will

Be recorded in the House files and used to ensure the students' health and safety. If you get a new mobile phone number, please let house staff know immediately.

Contact with House Staff will always be through the House mobile or School landline.

Students may access Video on Demand Platforms, (eg. Netflix, Amazon Prime etc.), on their personal device. However, appropriate parental controls are required to be set by parents so that only age-appropriate material can be viewed.

Personal games consoles cannot be connected to the School's network. The School provides consoles in the student common areas for use by the students.

Virtual Private Networks, (VPNs) must never be used. Any attempt to circumvent the school network filtering and monitoring software will result in loss of phone privileges.

7. Education

The School aims to teach all students to understand why they need to behave responsibly if they are to protect themselves. Discussions take place in academic classes, in PSHE, in boarding houses and through assemblies on the safe use of the Internet and social media. The school engages with the local police who visit both sites to educate students about online safety.

a. Working with parents

The School seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will contact parents if there are concerns about a student's behaviour and encourages parents to share concerns with the school. Parents are provided with Government guidance on safety in the online environment by the Designated Safeguarding Lead.

b. 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: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/