RIKKYO SCHOOL IN ENGLAND

ICT Acceptable Use Policy

Date	Review Date	Coordinator	Headmaster
March 2021	March 2022	Mr.T.Okuno	Dr. T. Okano

Scope of this policy

1. Introduction

1.1. Rikkyo School in England is committed to protecting its pupils from illegal or damaging use of technology by individuals, either knowingly or unknowingly.

1.2. As users of the School's IT services pupils have a right to use its computing services; that right places responsibilities on these users which are outlined below. Misuse of the computing facilities in a way that constitutes a breach or disregard of the following policy may also be in breach of other School policies.

1.3. Ignorance of this policy and the responsibilities it places on users is not an excuse in any situation where it is assessed there has been a breach of the policy and its requirements.

1.4. Pupils who connect their own IT equipment to the School's network and the services available (including the use of mobile network) are particularly reminded that such use requires compliance to this policy.

1.5. Pupils are directed to this policy during their induction and are required to acknowledge their agreed adherence to and compliance with the policy when they first log on to the network.

1.6. A copy of this policy is available to parents on request and on the school website and the School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote the safe use of technology.

2. Purpose

2.1. The purpose of this policy is to:

2.1.1. outline the acceptable and unacceptable use of computer equipment or "online services" owned by the School, and acceptable or unacceptable general behaviour in ICT areas;

2.1.2. educate and encourage pupils to make good use of the educational opportunities presented by access to technology;

2.1.3. safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:

2.1.3.1. exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);

2.1.3.2. the sharing of personal data, including images;

2.1.3.3. inappropriate online contact or conduct; and

2.1.3.4. cyberbullying and other forms of abuse;

2.1.4. help pupils take responsibility for their own safe use of technology (i.e. limiting the risks that children and young people are exposed to when using technology);

2.1.5. ensure that pupils use technology safely and securely and are aware of both external and peer to peer risks when using technology.

2.2. These rules are in place to protect pupils and the School. Inappropriate use exposes the School and its academic partners to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

3.1. This policy applies to all pupils within the Rikkyo School.

3.2. The School will take a wide and purposive approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including:

3.2.1. The internet
3.2.2. Email
3.2.3. Mobile phones
3.2.4. Desktops, laptops, netbooks, tablets etc
3.2.5. Personal music players
3.2.6. devices with the capability for recording and / or storing still or moving images
3.2.7. social networking, blogging and other interactive web sites
3.2.8. instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards, conference meetings (including Zoom, Google Meet and Hangouts)
3.2.9. webcams, video hosting sites (such as YouTube, Twitch, Mixer)
3.2.10. gaming sites
3.2.11. Virtual Learning Environments (such as Google Classroom, GSuite for Education)
3.2.12. SMART boards and interactive boards
3.2.13. other photographic or electronic equipment e.g. GoPro devices and other wearable technology.

3.3. This policy applies to the use of technology on School premises.

3.4. This policy also applies to the use of technology off school premises if the use involves staff and any member of the School community or where the culture or reputation of the School or member of staff are put at risk.

4. Safe use of technology

4.1. We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.

4.2. The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

4.3. Pupils may find the following resources helpful in keeping themselves safe online: http://www.thinkuknow.co.uk

http://www.childnet.com
https://www.childline.org.uk/

4.4. School network is filtered and security rules are applied to all devices connected to the School WiFi. There are restrictions put in place for each device.

5. Procedures

5.1. Pupils are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If a pupil is aware of misuse by other pupils, should talk to a teacher about it as soon as possible.

5.2. Any misuse of technology by pupils will be dealt with under the School's Pupil Behaviour and Discipline Policy.

5.3. Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-Cyber Bullying Policy. If a pupil thinks that he / she might have been bullied or that another person is being bullied, he / she should talk to a teacher about it as soon as possible. See the School's Anti-Cyber Bullying Policy for further information about cyberbullying and online safety.

5.4. In any case giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's Child Protection and Safeguarding policy). If a pupil is worried about something that he / she has seen on the internet, or on any electronic device, including on another person's electronic device, he / she must tell a teacher about it as soon as possible.

5.5. In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to the Channel programme, which focuses on support at an early stage to people who are identified as being vulnerable.

5.6. In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead and the Director of ICT who will record the matter centrally.

6. Unacceptable Usage

6.1. The School provides internet access and an email system to pupils to support their academic progress and development.

6.2. Unacceptable use of School technology and network resources may be summarised as, but not restricted to:

6.2.1. Actions which cause physical damage to any ICT hardware, including peripherals (eg, mouse, cables, wiring, printers);

6.2.2. Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate;

6.2.3. Viewing, retrieving, downloading or sharing any offensive material which may include content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity;

6.2.4. Threatening, intimidating or harassing staff, pupils or others;

6.2.5. Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
6.2.6. Defamation;
6.2.7. Unsolicited advertising often referred to as "spamming";
6.2.8. Sending emails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address;
6.2.9. Attempts to break into or damage computer systems or data held thereon;
6.2.10. Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, eg use of equipment which is inadequately protected against viruses and spyware;
6.2.11. Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;
6.2.12. Using the School network for unauthenticated access;
6.2.13. Any other conduct which may discredit or harm the School, its staff, community or the ICT Facilities;
6.2.14. Using the ICT facilities for gambling;
6.2.15. Using the ICT facilities for carrying out any illegal trading activity.

6.3. This policy sets out the following rules and principles with which pupils must comply:
6.3.1. Authorisation - access and security
6.3.2. Use of the internet and email
6.3.3. Use of mobile electronic devices and
6.3.4. Photographs and images.

These principles and rules apply to all use of technology.

6.4. Anyone who mistakenly accesses inappropriate material should notify ICT Support.
6.5. The School may inform the police or other law enforcement agency in the event of any use that could be regarded as giving rise to criminal proceedings.

7. Sanctions

7.1. Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the School may apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Pupil Behaviour and Discipline Policy including, in the most serious cases, criminal prosecution. Other sanctions might include: verbal warning, increased monitoring procedures and withdrawal of the right to access the School's internet and email facilities. Any action taken will depend on the seriousness of the offence

7.2. Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with the practices and procedures in this policy and the School's policy on the searching and confiscation of electronic devices contained in the Anti-Cyber Bullying Policy and Searching, Screening and Confiscation Policy.

Key Principles and Rules

8. Authorisation - access and security

8.1. In order to use the School's ICT Facilities pupils must first be properly registered to use such services. Registration to use School services implies, and is conditional upon acceptance of this Acceptable Use Policy.

8.2. The registration procedure grants authorisation to use the core ICT Facilities of the School. Following registration, a username and password will be allocated to each pupil. Authorisation for other services may be requested by application to the Head of ICT Department.

8.3. Any attempt to access or use any user account or email address, for which the pupil is not authorised, is prohibited.

8.4. Pupils may not use, or attempt to use, ICT resources allocated to another person, except when explicitly authorised.

8.5. Pupils must take all reasonable precautions to protect the School's resources (including the ICT Facilities and the School's information and data), their username and passwords.

8.6. Purpose of Use

8.6.1. ICT facilities are provided primarily to facilitate a person's essential work as a pupil. Use for other purposes, such as personal email or recreational use of the Internet, is only permitted during the permitted times specified by the School and is a privilege, which can be withdrawn at any time and without notice. Any such use must not interfere with the pupil's studies or any other person's use of computer systems and must not, in any way, bring the School into disrepute.

8.6.2. School email addresses and associated School email systems must be used for all official School business. All pupils must regularly read their School email and delete unwanted or unnecessary emails at regular intervals.

8.7. The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. Pupils must not try to bypass this filter.

8.8. Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If a pupil thinks or suspects that an attachment, or other downloadable material, might contain a virus, he / she must speak to a member of ICT Support staff before opening the attachment or downloading the material. Pupils must not disable or uninstall anti-virus software on the School's computers.

8.9. Privacy and Monitoring

8.9.1. All allocated usernames, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. Pupils are personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be shared with any other person.

8.9.2. Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.

8.9.3. For the protection of all pupils, their use of email and of the internet when accessed via the School network will be monitored by the School. Pupils should

remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private

8.9.4. Pupils must not interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly pupils must not make unauthorised copies of information belonging to another user. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.

9. Use of the internet and email

9.1. The School does not undertake to provide continuous internet access. Email and website addresses at the School may change from time to time.

9.2. Use of internet

9.2.1. Pupils must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently

9.2.2. Pupils must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. Pupils must tell a member of staff immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

9.2.3. Pupils must not communicate with staff using social networking sites or other internet or web based communication channels unless this is an educational platform which has been approved by the Headmaster, (such as G Suite).

9.2.4. Pupils must not bring the School into disrepute through their use of the internet.

9.2.5. Copyright Compliance

9.2.5.1. All pupils must abide by laws relating to the use and protection of copyright.

9.2.5.2. Pupils must not download, copy or otherwise reproduce material for which they have not obtained permission from the relevant copyright owner. If such material is required for any purpose eg research then copyright permission must be obtained and documented before such material is used.

9.2.5.3. Pupils are reminded that the School treats plagiarism very seriously and will investigate any allegation i.e. the intentional use of other people's material without attribution.

9.3. Use of email

9.3.1. Pupils must use their School email accounts for any email communication with staff. Communication either from a personal email account or to a member of staff's personal email account is not permitted.

9.3.2. Email should be treated in the same way as any other form of written communication. Pupils should not include or ask to receive anything in an email which is not appropriate to be published generally or which they believe the School or their parents would consider to be inappropriate. Remember that emails could be forwarded to or seen by someone they did not intend.

9.3.3. Pupils must not send or search for any email message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If they are unsure about the content of a message, they must speak to a member of staff. If they come across such material they must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

9.3.4. Pupils must not read anyone else's emails without their consent.

10. Use of mobile electronic devices

10.1. "Mobile electronic devices" includes but is not limited to mobile 'phones, smartphones, tablets, laptops and MP3 players

10.2. Pupils who are permitted to use their mobile electronic devices may use their devices on the Student Wi-Fi network only. Pupils are not permitted at any time to connect devices with a network cable in any part of the School or to any other school Wi-Fi network.

10.3. Pupils are not allowed to use a mobile phone in school.

10.4. Pupils must not communicate with a member of staff's personal (as opposed to School) mobile phone except when this is expressly permitted by a member of staff (e.g. if a staff member has no school mobile and communication is required for the normal running of School business). For example this may on occasion be necessary during an educational visit. Any such permitted communications should be brief and courteous.

10.5. Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not they are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use and the School's safeguarding procedures will be followed in appropriate circumstances

10.6. Mobile electronic devices may be confiscated in appropriate circumstances. Pupils may also be prevented from bringing a mobile electronic device into the School temporarily or permanently.

10.7. The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

11. Photographs and images

11.1. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

11.2. Pupils may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.

11.3. Pupils must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.

11.4. The posting of images which in the reasonable opinion of the School is considered to be offensive or which brings the School into disrepute on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

11.5. For further regulations, please refer to Photographic and Video Images and Audio Recordings Policy.

12. Responsibilities

12.1. This policy is the responsibility of the ICT Committee.

12.2. Role of the Headmaster and Senior Leadership Team

The Headmaster and the Senior Leadership Team has appointed a member of staff to be responsible for ICT and E-Safety and will:

- ensure all school personnel are aware of and comply with this policy;
- ensure all school personnel sign and date the 'Acceptable Use of ICT Agreement';
- work closely with the coordinator;
- provide guidance, support and training to all staff;
- make effective use of relevant research and information to improve this policy;
- monitor the effectiveness of this policy

12.3. Role of the Coordinator

The Coordinator will:

- lead the development of this policy throughout the school;
- work closely with the Headmaster;
- devise and update when appropriate acceptable use guidelines;
- provide guidance and support to all students and staff;
- keep a log of all ICT equipment used by school personnel;
- make effective use of relevant research and information to improve this policy;
- keep up to date with new developments and resources;
- undertake risk assessments when required;
- review and monitor devices used on schools network.

12.4. Role of School Personnel

School personnel will:

- comply with all aspects of this policy;
- be aware of all other linked policies;
- sign and date the 'Acceptable Use of ICT Agreement';
- be aware of the acceptable use guidelines;
- protect their username and passwords;

log off when finished using a computer.

RIKKYO SCHOOL IN ENGLAND

Appendix 1

ICT Services Acceptable Use Policy (AUP) Summary for Students

Your agreement to abide by the following guidelines ensures your safety and the efficient functioning of the School's IT facilities:

1. Definition

The ICT facilities at Rikkyo School are defined as computers, tablets, laptops, Chromebooks, software, peripherals and any other electronic device or item. Internet and G Suite which includes, but is not limited to: Gmail, Docs, Slides, Sheets, Forms, Classroom are included as ICT facilities. It also applies to any device of your own which you are authorised to connect to the School wifi network.

2. Software

You may not install software on any school machine or any device owned or managed by the school.

3. Passwords

3.1. Keep your password safe and never share your login details. All passwords identify you on the system and if anyone uses your password, it will be traced back to you.

3.2. You should use a strong password i.e. one which includes one capital, number and symbol. You should regularly change your password.

3.3. If you suspect someone else knows your password, you should change it immediately.

4. Storage areas

You are responsible for the file management of your storage area on your G Suite account. This should be used only for saving school work.

5. Right to review

The School has the right to review any files and communications to ensure that you are using the system responsibly.

6. The internet

The Internet is provided for you to conduct research and school-related work. Access requires responsibility; it is a privilege not a right. Your teachers will guide you toward appropriate materials. Internet and email activity is monitored and the IT Department is authorised to review internet usage history if required.

7. Emails and messaging

7.1. You will be provided with a School Gmail account for accessing G Suite (including Google Classroom) and for communications between you and your teachers.

7.2. Use of your own external email is not allowed for school communication.

7.3. You are allowed to contact other students via the School G Suite account.

8. Social Network

The use of social network websites in School is not permitted. When using social network sites at home, you must not post any insulting or offensive material of any kind about other students, teachers or the School. You must not post any photographs or videos of anyone without their permission.

9. Use of mobile phones

9.1. The School does not allow you to use your mobile phone on School premises.

10. Unacceptable use of IT

The following will be dealt with in the same way as any other form of unacceptable behaviour in school:

10.1. Sending or displaying any offensive material (e.g. messages, pictures or videos).

10.2. Recording or taking photographs or video footage of anyone without their permission.

10.3. Using inappropriate language, insulting or harassing others.

10.4. Damaging computers, computer systems or networks.

10.5. Offensive messages sent from mobile phones or any other device.

10.6. Using other students passwords and trespassing in other people's folders.

This list is not exhaustive and behaviour that is deemed inappropriate will be dealt with on a case-by-case basis.

If you have any issues or concerns regarding the misuse of ICT you should report your concerns to the ICT Systems Manager or any member of staff.

11. Sanctions

Breaking the above rules will result in a temporary or permanent ban on Internet or computer use. Additional disciplinary action may be taken if the offence is serious.