# RIKKYO SCHOOL

# ACCEPTABLE USE POLICY

**This policy applies to the whole school**

*The Policy is available to the school staff via Staff Share*

**We have a whole school approach to safeguarding, which is the golden thread that runs throughout every aspect of the school. All our school policies support our approach to safeguarding (child protection). Our fundamental priority is our children and their wellbeing; this is first and foremost.**

**Scope:** All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours, including activities away from school. All new employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the *Policies Register*.

**Legal Status:** Complies with The Education (Independent School Standards) (England) Regulations and the National Minimum Standards (NMS) for Boarding Schools, currently in force.

**Monitoring and Review:** These arrangements are subject to continuous monitoring, refinement, and audit by the Headmaster. The Board of Governors will undertake a full annual review of this document, inclusive of its implementation and the efficiency with which the related duties have been implemented. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed arrangements and it will be made available to them in writing or electronically.

Signed:

Policy Agreed: September 2024
Date Published: September 2024
Next Review: September 2025

Dr T Okano
Headmaster

Mr J Sugiyama
Chair of Governors

## Scope of this Policy

This policy applies to all members of the school community (staff or pupils) who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

## Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.

- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).

- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.

- Do not access or share material that infringes copyright, and do not claim the work of others as your own.

- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

### Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.

- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.

- Do not attempt to install software on, or otherwise alter, school IT systems.

- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

### Passwords

Passwords protect the school's network and computer system are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

### Use of Property

Any property belonging to the school should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the Bursar.

### Use of school systems

The provision of School email accounts, Wi-Fi and internet access is for official School business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT

use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

### Use of personal devices or accounts and working remotely

All official school business of staff, Trustees, and Governors must be conducted on School systems, and it is not permissible to use personal email accounts for School business. Any use of personal devices for School purposes, and any removal of personal data or confidential information from School systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Bursar.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, including two-factor authentication[1], encryption etc.

### Monitoring and access

Staff, parents and pupils should be aware that School email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the School where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether such devices are permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

### Tracking Devices and Technology

The school is not responsible for individual settings on personal devices, nor for the use of tracking apps / devices for purely personal and domestic purposes.

Use of this technology in the context of school activities is not specifically encouraged but if parents do plan to use it then they should be aware of potential third party privacy considerations and only use it for domestic / personal purposes in respect of their own child and/or their or their child's belongings.

### Compliance with related school policies

To the extent they are applicable to you, you will ensure that you comply with the school's Online Safety Policy, Acceptable Use of Mobile 'Phones, Monitoring & Filtering Standards, Remote Learning Policy, and Email Policy.

### Retention of digital data

Staff and pupils must be aware that all emails sent or received on school systems will be routinely deleted after two years and email accounts will generally be closed and the contents deleted within one year of that person leaving the school.

Any information from email folders that is necessary for the school to keep for longer, including personal information (e.g. for a reason set out in the school privacy notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

[1] When installed

If you consider that reasons exist for the protocol not to apply or need assistance in how to retain and appropriately archive data, please contact the Bursar.

### Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or students become aware of a suspected breach, they should report it immediately to the Bursar or Headmaster if the Bursar is not available.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

### Use of Artificial Intelligence

Please refer to the School's AI Policy.

### Breaches of this policy

A deliberate breach of this policy by staff or pupils will be dealt with as a disciplinary matter using the school's usual applicable procedures. In addition, a deliberate breach by any person may result in the school restricting that person's access to school IT systems.

If you become aware of a breach of this policy or the Online Safety Policy, or you are concerned that a member of the School community is being harassed or harmed online you should report it to the DSL. Reports will be treated in confidence wherever possible.