RIKKYO SCHOOL IN ENGLAND

Acceptable Use of ICT

Date	Review Date	Coordinator	Headmaster
16/04/2019	01/10/2019	Mr.T.Okuno	Dr. T. Okano

We believe this policy relates to the following legislation:

- Computer Misuse Act 1990
- Misuse of Information Act 1990
- Health and Safety (Display Screen Equipment) Regulations 1992
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Equality Act 2010
- Counter Terrorism and Security Act 2015

The following documentation is also related to this policy:

- Data Protection and Security: A Summary for Schools (Becta 2004)
- The Safe Use of New Technologies (Ofsted)
- Prevent Strategy (HM Gov)
- Teaching approaches that help build resilience to extremism among people (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children

We believe information and communications technology includes all forms of computing, the internet, telecommunications, digital media and mobile phones. School personnel have clear responsibilities with regard to the use of all ICT equipment and ICT facilities.

Any member of the school personnel that uses illegal software or access inappropriate websites when in school faces dismissal. All school personnel will be made aware of all legislation relating to computer misuse, data protection and copyright.

We expect all school personnel to sign and date the 'Acceptable Use of ICT Agreement' and be fully aware of and implement the internet safety policy. All school personnel have the duty to report any misuse of the ICT equipment or the ICT facilities of this school.

We have a duty to ensure the internet safety of all pupils within this school.

We have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremists groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. Periodic risk assessments are undertaken to assess the risk of pupils being drawn into terrorism. School personnel must be aware of the increased risk of online radicalisation, and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

We are aware that under the 'Counter-Terrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent duty and we believe it is essential that school personnel are able to identify those who may be vulnerable to radicalisation or being influenced by extremist views, and then to know what to do when they are identified.

We provide a safe environment where we promote pupils' welfare. Within this environment we work hard to build pupils' resilience to radicalisation and extremism by promoting fundamental British values and for everyone to understand the risks associated with terrorism. We want pupils to develop their knowledge and skills in order to challenge extremist views.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

Aims

- To ensure school personnel are aware of all legislation relating to computer misuse, data protection and copyright.
- To share good practice within the school.
- To protect children from the risk of radicalisation and extremism.
- To ensure compliance with all relevant legislation connected to this policy.

Responsibility for the Policy and Procedure

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.

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.

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 user name and passwords;
- log off when using a computer.

Procedures for dealing with Inappropriate/Illegal Internet Access or Material

If staff or pupils discover unsuitable websites, this should be immediately reported to your class teacher or line manager, they in turn will report any issues to the Headmaster who will consider a referral to the Internet Watch Foundation (IWF) and the Police. Illegal material within the school's network is a very serious situation and must always be reported to the Police.
Our school ensures processes are in place to minimise the risk of students gaining access to inappropriate materials, through supervision and monitoring. Any incident that involves inappropriate adult access to illegal material on the school premises will be dealt with by the school's disciplinary policy.

What to do in the event of discovery of illegal material

- Seek immediate and specific advice from your Class Teacher or Line Manager who will consult with the Headmaster.

- Prevent any further physical access to the device until the correct advice is gained.

- **Unless absolutely necessary, DO NOT remove the power from a working PC and definitely DO NOT start a PC if it is already turned off.**

- Consider if it is necessary to prevent remote access to the device.

- If you believe that a member of staff or pupil who has left the site, could remove or damage evidence on the device remotely, unplug **ONLY** the network cable from the back of the device to prevent this access from taking place.

- If the PC is already turned off and it is no longer realistically possible to prevent further physical access to the device (i.e. lack of supervision, high levels of access or an unoccupied location) **disconnect the power at the base unit (not the wall)** and remove

the battery from a laptop. Store this device securely in a location where no one else can gain access to it and make a note of the date, time and name of the individual who performed this action.

Under no circumstances should you attempt to conduct an investigation of your own or bring in an outside expert to do so as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

Combating Cyber-bullying

Cyber-bullying can be defined as 'the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else'. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages, the size of the audience, perceived anonymity, and even the profile of the person doing the bullying and their target.

Cyber-bullying takes different forms: threats and intimidation, harassment or 'cyberstalking'(e.g. repeatedly sending unwanted texts or instant messages), vilification /defamation; exclusion or peer rejection, impersonation, unauthorised publication of private information or images and manipulation.

Some cyber-bullying is clearly deliberate and aggressive, but it is important to recognise that some incidents of cyber-bullying are known to be unintentional and the result of simply not thinking about the consequences. What may be sent as a joke may not be received as one, and indeed the distance that technology allows in communication means the sender may not see the impact of the message on the receiver. There is also less opportunity for either party to resolve any misunderstanding or to feel empathy. It is important that pupils are made aware of the effects of their actions.

In cyber-bullying, bystanders can easily become perpetrators, e.g. by passing on or showing to others images designed to humiliate, or by taking part in online polls or discussion groups. They may not recognise themselves as participating in bullying, but their involvement compounds the misery for the person targeted. It is recommended that anti-bullying policies refer to those 'bystanders' — better termed 'accessories' in this context — who actively support cyber-bullying and set out sanctions for this behaviour.

It is important that pupils are aware that their actions have severe and distressing consequences, and that participating in such activity will not be tolerated.

There are particular features of cyber-bullying that differ from other forms of bullying which need to be recognised and taken into account when determining how to respond effectively. The key differences are:

- **Impact** — the scale and scope of cyber-bullying can be greater than other forms of bullying.
- **Targets and perpetrators** — the people involved may have a different profile to traditional bullies and their targets.
- **Location** — the 24/7 and any-place nature of cyber-bullying.
- **Anonymity** — the person being bullied will not always know who is attacking them.
- **Motivation** — some pupils may not be aware that what they are doing is bullying.
- **Evidence** — unlike other forms of bullying, the target of the bullying will have evidence of its occurrence.

Prevention

We seek to instil values in all members of the School, which should, ideally, preclude all bullying. These are reinforced by a PSHE programme which requires the School to spend time talking to students about cyber-bullying and its effects and consequences. In essence, these seek to inculcate respect for others, their property and their individuality. We hope these values underpin ordinary curricular lessons too.
It is crucial to the School's success in dealing with cyber-bullying that all students and staff are made aware that it is unacceptable and should not be tolerated. It is the responsibility of all students and staff to take action if they are aware of it happening. To remain silent is to condone the action of the bully.

Process

Information is crucial in dealing with the problem. Those who feel that they are being bullied, or who are witnesses to what they believe is bullying/cyber-bullying, should always tell a member of staff.
Advice, support and counselling will be offered to all parties involved, and, if necessary, their parents. While recognising that both victim and bully need help, we do not adopt a 'no blame' position.

1. If a pupil receives an abusive e-mail or text, they should report the matter to a member of staff as soon as possible. A copy of the e-mail with full headers, plus dates and times should be saved. Staff will investigate all complaints of abuse and take action accordingly.
2. Depending on the nature of the allegation, the case will be taken up either by the Headmaster or Deputy Headmaster or a combination of these two. As a rough guide, the more serious the allegation, the more likely it is to involve senior staff and/or the Police.
3. Interviews will be conducted fairly, giving all sides the opportunity to state their case, so as to establish the truth in what seldom turn out to be straightforward issues. In all cases, pupils will be warned not to do or say anything that may prejudice their position vis-à-vis the pupil who has been bullied. (No revenge/stirring up support among friends, no taking the law into their own hands.)

4. Except for the most straightforward cases, in which truth has been established and the matter has been resolved swiftly, an interview will be conducted; a pupil would be invited to bring a friend or member of staff to support them in any such interview. This will enable a record to be kept of the interview, and what is said, to be corroborated. Notes, both rough copies and, where necessary, a brief summary and copies of any letters sent to parents will be put on files with cross referencing where appropriate.
5. Letters written to parents will detail the nature of the offence and any sanctions imposed, and will set out what improvements the School expects to be made in behaviour as well as the consequences of failure to improve. Recommendations may be made about visits for professional help e.g. counselling for everyone involved.
6. At the conclusion of the investigation, if appropriate, one of the members of staff involved will contact parents of all pupils directly involved and inform them of action taken. Wherever possible, the identity of “informers” and pupils other than the son or daughter of the parent will not be disclosed.
7. In practice, the sanctions applied range from a verbal warning or a ban on use of the School’s computer network, to temporary or permanent exclusion, depending on the gravity of the offence and the pupil’s previous record with reference to bullying.

Sanctions

In practice, the sanctions applied range from a verbal warning or a ban on use of the School’s computer network to a temporary or permanent exclusion, depending on the gravity of the offence and the pupil’s previous record with reference to bullying / cyberbullying. In the most severe cases, it can result in criminal prosecution.

The aim of sanctions is to:

- Help the person harmed to feel safe again and be assured that the bullying will stop.
- Hold the perpetrator to account getting them to recognise the harm caused and deter them from repeating the behaviour.
- Demonstrate to the school community that cyber-bullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving similarly.

Cyber-bullying will have an impact on the education and wellbeing of the person being bullied, and the physical location of the bully at the time of their action is irrelevant in this. Schools now have broad new powers to discipline and regulate the behaviour of pupils, even when they are off the school site. Misconduct of any kind outside of school will be amenable to school discipline if the welfare of another pupil or the culture or reputation of the college are placed at risk.

RIKKYO SCHOOL IN ENGLAND

Anti-Cyber-bullying Code: Advice to pupils

Being sent an abusive or threatening text message, or seeing nasty comments about yourself on a website, can be really upsetting. This code gives you seven important tips to protect yourself and your friends from getting caught up in cyber-bullying, and advice on to how to report it when it does happen.

1. Always respect others
Remember that when you send a message to someone, you cannot see the impact that your words or images may have on the other person. That is why it is important to always show respect to people and be careful what you say online or what images you send. What you think is a joke may really hurt someone else. Always ask permission before you take a photo of someone.
If you receive a rude or nasty message or picture about someone else, do not forward it. You could be assisting a bully and even be accused of cyber-bullying yourself. You could also be breaking the law.

2. Think before you send
It is important to think before you send any images or text about yourself or someone else by email or mobile phone, or before you post information on a website. Remember that what you send can be made public very quickly and could stay online forever. Do you really want your teacher, parents or future employer to see that photo?

3. Protect your password
Don't let anyone know your passwords. It is a good idea to change them on a regular basis. Choosing hard-to-guess passwords with symbols or numbers will help stop people hacking into your account and pretending to be you. Remember to only give your mobile number or personal website address to trusted friends.

4. Block the Bully
Most responsible websites and services allow you to block or report someone who is behaving badly. Make use of these features, they are there for a reason!

5. Don't retaliate or reply
Replying to bullying messages, particularly in anger, is just what the bully wants.

6. Save the evidence
Learn how to keep records of offending messages, pictures or online conversations.
These will help you demonstrate to others what is happening and can be used by your school, internet service provider, mobile phone company, or even the police to investigate the cyber-bullying.

7. Make sure you tell
You have a right ***not*** to be harassed and bullied online. There are people that can help:

- Tell an adult you trust who can help you to report it to the right place, or call a helpline like ChildLine on 0800 1111 in confidence.
- Tell the provider of the service you have been bullied on (e.g. your mobile phone operator or social-network provider). Check their websites to see where to report.
- Tell your teacher, the boarding staff or any member of staff. They will support you and can discipline the person bullying you.

Conclusion

- E-mails should contain the same professional levels of language and content that apply to letters.
- Students should not give out any information relating to themselves or the School to an unknown individual without specific permission of a member of staff.
- Staff or students found using the Internet unprofessionally or inappropriately, as defined by the Statement of Acceptable Internet Use will be banned temporarily or permanently from using it and in addition disciplinary action may be added in line with existing School practices.
- The School reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited along with any e-mail sent or received.

The Internet provides a huge source of information and a fast convenient means of communication. Information gained from the Internet may be inaccurate or biased. Used properly, it can provide excellent resources, however, the systems is open to abuse and there are many problems that need to be overcome to ensure safe effective "surfing".

The School's current Internet Service Provider will filter out unpleasant material.

Training

All school personnel:

- have equal chances of training, career development and promotion
- receive periodic training so that they are kept up to date with new information

Monitoring the Effectiveness of the Policy

The practical application of this policy will be reviewed annually or when the need arises by the coordinator and the Headmaster.

Previous dated 22/01/2016
Reviewed 11/01/2017, 08/05/2018, 01/10/2018

RIKKYO SCHOOL IN ENGLAND

Acceptable ICT Use Agreement – School Personnel

I understand that the school Internet facility is for the good of my professional development, for the development of this school and must be used only for educational purposes.

I realise that I have a personal responsibility to abide by the set rules and regulations when using the Internet and I am aware of the consequences if I breach them.
I am aware that by beaching the rules and regulations it may lead to:

- withdrawal of my user access
- the monitoring of how I use the Internet
- disciplinary action
- criminal prosecution

I will report immediately to the E-Safety Coordinator any accidental access to inappropriate material or websites that I may have accessed.

I will log on to the Internet by using my password, which will be changed at regular intervals.

When using the school's Internet I will not:

- use the Internet in such a way that it will bring the school into disrepute
- use inappropriate or illegal websites
- download inappropriate material or unapproved software
- disrupt the time of other Internet users by misusing the Internet
- use inappropriate language
- use language that may provoke hatred against any ethnic, religious or other minority group
- produce, send out, exhibit or publish material that will cause offence to anyone
- divulge any personal information about myself, any other user or that of pupils
- divulge my login credentials or passwords to anyone
- use the login credentials or passwords of any other user
- use a computer that is logged on by another user
- use any social networking site
- transfer the images of pupils without prior permission of the Headmaster and from parents
- use email for private use but only for educational purposes
- compromise the Data Protection Act or the law of copyright in any way

I agree to abide by this agreement.

Employee Name:		**Headmaster Name:**	
Employee Signature:		**Headmaster Signature:**	
Date:		**Date:**	

RIKKYO SCHOOL IN ENGLAND