RIKKYO SCHOOL IN ENGLAND

E-Safety

Date	Review Date	Coordinator	Headmaster
26/02/2020	26/02/2021	Mr.T.Okuno	Dr. T. Okano

We believe this policy relates to the following legislation:

- Obscene Publications Act 1959
- Children Act 1989
- Computer Misuse Act 1990
- Police Act 1997
- Data Protection Act 2018
- Human Rights Act 1998
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- Education Act 2003
- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Children and Young Persons Act 2008
- School Staffing (England) Regulations 2009
- Equality Act 2010
- Education Act 2011
- Protection of Freedoms Act 2012
- Counter Terrorism and Security Act 2015

The following documentation is also related to this policy:

- Dealing with Allegations of Abuse against Teachers and other Staff: Guidance for Local Authorities, Headmasters, School Staff, Governing Bodies and Proprietors of Independent Schools (DfE)
- Equality Act 2010: Advice for Schools (DfE)
- Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges (DfE)
- 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

School personnel, parents and pupils should be aware that school email and internet usage will be monitored for safeguarding, conduct and performance purposes. Web history and school email accounts may be accessed by the school where necessary for a lawful purpose.

RIKKYO SCHOOL IN ENGLAND

This E-Safety policy is one element within our overall school arrangements to Safeguard and Promote the Welfare of all Children in line with our statutory duties.

We believe that used correctly Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems.

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security. E-Safety, which encompasses Internet technologies and electronic communications such as mobile phones, ipods, ipads and wireless technology, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We believe all pupils and other members of the school community have an entitlement to safe Internet access at all times.

We have a duty to safeguard children, young people and families from violent extremism. School personnel must be aware of the increased risk of online radicalisation, and alert to changes in pupil's behaviour. Any concerns need to be reported to the Designated Safeguarding Lead.

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 provide pupils with quality Internet access as part of their learning experience across all curricular areas.
- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet.
- To evaluate Internet information and to take care of their own safety and security.
- To raise educational standards and promote pupil achievement.
- To protect children from the risk of radicalisation and extremism.
- To ensure compliance with all relevant legislation connected to this policy.
- To work with other schools and the local authority to share good practice in order to improve this policy.

Internet Filtering and Use

We have a contract with a reputed Internet provider to manage a secure and filtered Internet service which enables us to safely access and use the Internet and all email. The Internet filtering service will be annually reviewed.

Access to the Internet is designed to protect pupils and school personnel by blocking the following content:

☐ adult content containing sexually explicit images
☐ violent content containing graphically violent images
☐ hate material content promoting violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
☐ illegal drug taking content relating to the use or promotion of illegal drugs or the misuse or prescription drugs
☐ criminal content relating to the promotion of criminal and other activities
☐ gambling content relating to the use of online gambling websites
☐ non educational websites such as social networking sites

All users access the Internet in accordance with the School's Acceptable Internet Use & Agreement and will inform the ICT coordinator if at any time they find they have accessed inappropriate Internet sites.

When inappropriate material has been accessed the Internet Service Provider will be contacted and if necessary the Police.

Responsibility of the Policy and Procedure

Role of the Headmaster

The Headmaster has appointed a member of staff to be responsible for E-Safety and will:

- ensure the safety and E-Safety of all members of the school community;
- in conjunction with the Senior Leadership Team will ensure all school personnel, pupils and parents are aware of and comply with this policy;
- work closely with the coordinator to create a safe ICT learning environment by having in place:
  - an effective range of technological tools
  - clear roles and responsibilities
  - safe procedures
  - a comprehensive policy for pupils, staff and parents
- ensure all new programs will be installed onto the network or stand alone machines by a reputable IT firm;
- ensure personal CD's and other data record devices may not be used in school;
- ensure everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence;
- investigate, record and report all infringements to e-safety by any member of staff or by a pupil;
- deal with all complaints of Internet misuse by school staff or pupils;

- ensure all pupils and staff read and sign the "Acceptable ICT Use Agreement" before using any school IT resource;
- ensure parents sign a consent form before their child has access to the Internet
- ensure an up to date record is kept of all pupils and staff who have Internet access
- inform parents if their child has misused the Internet;
- ensure a safe and secure username/password system is in place for all:
  - ☐ technical systems
  - ☐ networks
  - ☐ devices and
  - ☐ email and Virtual Learning Environments
- ensure all users are responsible for:
  - ☐ the security of their username and password
  - ☐ not allowing other users to use this information to access the system
  - ☐ reporting any suspicion or evidence that there has been a breach of security
  - ☐ changing their passwords at regular intervals
- deal with all breaches of security
- impose the appropriate sanctions to any infringement of e-Safety
- will immediately suspend a member of the school personnel if they commit an exceptionally serious act of gross misconduct
- ensure any inappropriate websites or material found by pupils or staff will be reported to the e-Safety Coordinator who will report it to the Internet Service Provider
- ensure the school website complies with current DfE guidelines
- ensure the following will not be published on the school website:
  - ☐ staff or pupils contact details
  - ☐ pictures of children without the written consent of the parent/carer
  - ☐ the names of any pupils who are shown
  - ☐ children's work without the permission of the pupil or the parent/carer
- make effective use of relevant research and information to improve this policy
- provide guidance, support and training to all staff
- monitor the effectiveness of this policy by:
  - ☐ monitoring learning and teaching by observing lessons
  - ☐ monitoring planning and assessment
  - ☐ speaking with pupils, staff and parents
- ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- embed E-Safety in all aspects of the curriculum and other school activities;
- ensure this policy is maintained and updated regularly.

Role of the E-Safety Coordinator

The coordinator will:

- be responsible for the day to day E-Safety issues;
- undertake an annual E-Safety audit in order to establish compliance with Local Authority guidance;

- ensure that all Internet users are kept up to date with new guidance and procedures;
- ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- undertake risk assessments in order to reduce Internet misuse;
- maintains a log of all E-Safety incidents;
- reports all E-Safety incidents to the Headmaster;
- ensure E-Safety is embedded in all aspects of the curriculum and other school activities;
- regularly update the school website with E-Safety information for parents;
- develop an internet safety curriculum for the whole school;
- lead the development of this policy throughout the school;
- work closely with the Headmaster;
- make effective use of relevant research and information to improve this policy;
- provide guidance and support to all staff;
- provide training for all staff on induction and when the need arises;
- keep up to date with new developments and resources;
- review and monitor.

Role of School Personnel

School personnel will:

- comply with all aspects of this policy
- any use of personal devices for school purposes such as private laptops and personal email accounts needs to be approved by the Head of Department;
- where permission is given for the use of personal devices, these must be used with appropriate safeguards: they need to be password protected and confidential information needs to be stored in a password protected file;
- USB sticks containing confidential data need to be encrypted if they are taken outside of the school;
- before using any Internet resource in school must accept the terms of the 'Acceptable Internet Use' statement;
- not allow others to use their login details for their computer except for staff of the IT Department
- report any suspicion that there has been a breach of security;
- ensure that they only use age appropriate material in the classroom;
- be responsible for promoting and supporting safe behaviours with pupils including password security;
- promote E-Safety procedures such as showing pupils how to deal with inappropriate material;
- report any unsuitable website or material to the Headmaster;
- will ensure that the use of Internet derived materials complies with copyright law;
- ensure E-Safety is embedded in all aspects of the curriculum and other school activities;
- undertake appropriate training;
- be aware of all other linked policies;

Role of Pupils

Pupils must not

- Take photos or videos of other pupils or staff without their permission.
- Take photos or videos in changing rooms, bathrooms, toilets will not be tolerated and will constitute a serious breach of discipline
- Take photos or videos of another person who is undressed or partly undressed will not be tolerated and will constitute a serious breach of discipline and possibly be a criminal offence
- Access social networking sites except those that are part of an educational learning platform and to newsgroups unless an identified need has been approved.

Pupils will be aware of this policy and will be taught to:

- be critically aware of the materials they read;
- validate information before accepting its accuracy;
- acknowledge the source of information used;
- use the Internet for research;
- respect copyright when using Internet material in their own work;
- report any offensive e-mail;
- report any unsuitable website or material to the E-Safety Coordinator;
- know and understand the school policy on the use of:
  - ☐ mobile phones
  - ☐ digital cameras
  - ☐ hand held devices
  - ☐ devices that connect to the internet

- know and understand the school policy on the taking and use of photographic images and cyber bullying;
- listen carefully to all instructions given by the teacher when using the internet.

Role of Parents/Carers

Parents/carers will:

- be aware of and comply with this policy;
- be asked to support the E-Safety policy and to sign the consent form allowing their child to have Internet access;
- make their children aware of the E-Safety policy;

Authorising Internet Access

- Before using any school ICT resource for accessing the internet, all pupils and staff must read and sign the 'Acceptable ICT Use Agreement'.
- Parents must sign a consent form before their child has access to the Internet.
- An up to date record will be kept of all pupils and school personnel who have Internet access.

Password Security

All users are responsible for the security of their username and password and must not allow other users to use this information to access the system. All breaches of security must be reported.

E-mail

Pupils must:

- only use approved e-mail accounts;
- report receiving any offensive e-mails;
- not divulge their or others personal details;
- not arrange to meet anyone via e-mail;
- seek authorisation to send a formal e-mail to an external organisation
- not take part in sending chain letters

School Website

Contact details on the website will be:

- the school address
- e-mail address
- telephone number

The school website will not publish:

- staff or pupils contact details;
- the pictures of children without the written consent of the parent/carer;
- the names of any pupils who are shown;
- children's work without the permission of the pupil or the parent/carer

Social Networking and Personal Publishing

Pupils will not be allowed access:

- to social networking sites except those that are part of an educational network or approved Learning Platform;
- to newsgroups unless an identified need has been approved

Inappropriate Material

- Any inappropriate websites or material found by pupils or school personnel will be reported to the E-Safety Coordinator who in turn will report to the Internet Service Provider.

Internet System Security

- New programs will be installed onto the network or stand alone machines by Local Authority technicians or a reputable IT firm;
- Personal CD players and other data record devices may not be used in school.
- Everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence.

Complaints of Internet Misuse

- The Headmaster will deal with all complaints of Internet misuse by school personnel or pupils.
- Parents will be informed if their child has misused the Internet.

Training

All school personnel will receive E-Safety training.

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/updated 11/01/2017, 30/11/2018, and 26/02/2020