Acceptable Use of ICT Policy for Pupils

This policy is applicable to all areas of the School including EYFS

Aims

- to educate and encourage pupils to make good use of the educational opportunities presented by access to technology;
- to safeguard and promote the welfare of pupils, in particular by anticipating and preventing risks arising from:

  - ✓ exposure to harmful or inappropriate material such as pornographic, racist, extremist or offensive materials;
  - ✓ the sharing of personal data including images;
  - ✓ inappropriate online contact or conduct;
  - ✓ cyberbullying and other forms of abuse.

- to minimise the risk of harm to the assets and reputation of the School;
- to help pupils take responsibility for their own safe use of technology;
- to ensure that pupils use technology safely and securely and are aware of both external and peer to peer risks when using technology;
- to prevent the unnecessary criminalisation of pupils.

Scope and Application

This policy applies to the whole school including the EYFS.

The policy applies to the use of technology at all times when a pupil is:

- in or at school
- representing the School or wearing School uniform;
- travelling to and from School
- on School organised trips;
- associated with the School at any time.

This policy shall also apply to pupils at all times and places in circumstances where failing to apply this policy may:

- affect the health, safety or well-being of a member of the School community or a member of the public;
- have repercussions for the orderly running of the School;
- bring the School into disrepute.

Regulatory Framework

This policy has been prepared to meet the School's responsibilities under:

Education (Independent School Standards) Regulations 2014;

Statutory framework for the EYFS (DfE March 2017);

Education and Skills Act;

Data Protection Act 2018 and GDPR;

Equality Act 2010.

This policy has regard to the following guidance and advice:

Keeping Children Safe in Education (DfE September 2018);

Preventing and Tackling Bullying (DfE July 2017);

Sexting in schools and colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety, August 2016);

Sexual violence and sexual harassment between children in schools and colleges (DfE May 2018);

Searching, screening and confiscation: advice for schools (DfE January 2018)

Publication and availability

This policy is available in hard copy on request. It is accessible on our web-site and is also available in large print.

Technology, Computing and Communication Devices

This policy relates to all technology, computing and communication devices, network hardware and software and services and applications associated with them including:

- the internet;
- email;
- mobile phones and smart phones;
- desktops, laptops, netbooks, tablets;
- personal music players;
- devices with capability for recording and/ or storing still or moving images;
- social networking and other interactive websites;
- instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards;
- webcams, video hosting sites, (such as YouTube);
- gaming sites;
- SMART boards;
- Other photographic or electronic equipment.

Safe Use of Technology

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

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. The safe use of technology is integral to the School's curriculum. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

Pupils may find the following resources helpful in keeping themselves safe online:

http://www.thinkuknow.co.uk

http://www.childnet.com/young-people

http://www.saferinternet.org.uk/advice-centre/young-people

http://www.disrespectnobody.co.uk

http://www.safetynetkids.org.uk

http://www.childline.org.uk/Pages/Home.aspx

The Internet

All pupils receive guidance on the use of the School's internet and they have their own unique log in. If a pupil is unsure about whether they are doing the right thing, they must seek assistance from a member of staff.

Pupils must follow school rules which form Appendix 1.

Procedures

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

Any misuse of technology will be dealt with under the School's behaviour and discipline policy.

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 Cyber-Bullying Policy. This applies to misuse of technology both within and outside school if it occurs between any pupil of Kirkstone House School.

The DSL takes lead responsibility within the School for safeguarding and child protection, including on-line safety. In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures.

In a case where the pupil is considered to be vulnerable to radicalisation, they may be referred to the Channel Programme.

I addition to following procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Headmistress who will record the matter centrally in the Technology Incidents Log.

Sanctions

Where a pupil breaches any of the school rules, the Headmistress will apply a sanction that is appropriate and proportionate to the breach in accordance with the School's Behaviour and Rewards and Sanctions Policies. In the most serious cases, this could be permanent exclusion.

Unacceptable use of technology could lead to the confiscation of a device or deletion of material in accordance with the School's policy on searching and retention and disposal of confiscated items.

If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police.

The School reserves the right to charge parents for any costs incurred to the School as a result of a breach of this policy.

Training

The School ensures that regular guidance and training is arranged so that staff know what is expected of them by this policy and have the necessary knowledge and skills to carry out their roles.

Record Keeping

All records created in accordance with this policy are managed with the law and the School's policies that apply to the retention and destruction of records.

All serious incidents involving the use of technology will be logged centrally in the Technology Incident Log by the Headmistress.

The records created in accordance with this policy may contain personal data. Staff must follow the School's data protection policies and procedures when handling personal data created in connection with this policy.

Authorised by	Mrs Corinne Jones Headmistress On behalf of the Proprietors
Dated	October 2018
Date of next review	October 2019

Appendix 1. Rules

1. Access to the internet from the School's computers and network must be for educational purposes only.

2. You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.

3. Use of any pupil laptop or other mobile device connected to the School's Wi-Fi is also covered by this policy regarding acceptable behaviour.

4. Passwords protect the School's network and computer system. You must not let anyone else know your password. If you believe that someone else knows your password, you must change it immediately.

5. You must not attempt to gain unauthorised access to anyone else's computer or to confidential information that you are not authorised to access. If there is a problem with your password, you must let the Headmistress' PA or your Computer Science teacher know immediately.

6. The School has a Firewall in place to ensure the safety and security of the School's networks. You must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the Firewall should be immediately reported to the Headmistress.

7. The School has filtering systems in place to block any unsuitable material wherever possible to protect the welfare and safety of pupils. No attempt must be made to bypass this.

8. Viruses can cause serious harm to the School network and that of others. Viruses are often spread through internet downloads or circulated as attachments to e-mails. If you suspect that an attachment or download may contain a virus, you must talk to the teacher in supervision immediately.

9. You must not disable any anti-virus software on the School's computers.

Appendix 2 Use of the internet and e-mail

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

2. You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself on line. This includes: full name, date of birth, address etc.

3. You should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights. You must not copy (plagiarise) another's work.

4. You must not view, retrieve, download or share any offensive material. Offensive materials include, but are 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 criminal offence. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

5. You must not communicate with staff using social networking sites or other internet or web based communication channels.

6. You must not bring the School into disrepute through your use of the internet. This includes uploading videos/pictures taken in school and of school events.

7. Email should be treated in the same way as any other form of written communication. You should not include or ask to receive anything in e-mail which is not appropriate to be published generally.