HAZELDENE SCHOOL

POLICY AND PROCEDURES FOR MONITORING EQUIPMENT AND APPROPRIATE ICT USE

REVISED SEPTEMBER 2016

SIGNED …… DATE……..
HEADTEACHER

SIGNED …… DATE …….
CHAIR OF GOVERNORS

POLICY AND PROCEDURES FOR MONITORING EQUIPMENT AND APPROPRIATE ICT USE

1. PURPOSE

1.1 The policy defines and describes the acceptable use of ICT (Information and Communications Technology) and all mobile devices for school-based employees. Its purpose is to minimise the risk to students of inappropriate contact from staff, to protect employees and schools from litigation and to minimise the risk to ICT systems.

2 SCOPE

2.1 This policy deals with the use of ICT equipment and services at Hazeldene and applies to all school-based employees.

3 SCHOOL RESPONSIBILITIES

3.1 Hazeldene School is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

3.2 The Headteacher/ICT Technician is responsible for maintaining an inventory of ICT assets (hardware and software), including any equipment issued to staff for personal use, such as a laptop, tablet or camera.

3.3 If a member of staff has reason to believe that any ICT equipment has been misused, s/he should consult the Headteacher without delay. Incidents will be investigated in a timely manner in accordance with agreed procedures.

4 USER RESPONSIBILITIES

4.1 Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. Staff must report all suspected breaches of this policy to the Headteacher.

4.2 Staff and their line managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.

4.3 By logging on to ICT systems, staff users agree to abide by this policy and other policies that relate to the use of ICT.

4.4 All users are expected to act in a responsible, ethical and lawful manner. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.

4.5 Staff provided with any portable ICT equipment, such as a laptop, tablet or camera, are expected to sign for its use on receipt. Staff may use school equipment for authorised business use only.

4.6 Staff must follow authorised procedures when taking mobile devices offsite.

4.7 No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws.

4.8 Users are required to protect their password and not utilise another user's account to misrepresent their identity for any reason.

4.9 Users must not take personal data (e.g. student data) away from the school without authorisation from the Headteacher. Any electronic data that is taken offsite must be password protected and encrypted. This includes data held on portable equipment (laptops, USB drives)

4.10 Any device connecting to the school network must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.

4.11 Within the terms of the Data Protection Act 1998 and Human Rights Act 1998, Hazeldene Lower School may record or inspect any information transmitted through or stored in its computers, including e-mail communications, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy.

- An account appears to be engaged in unusual or unusually excessive activity.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of ICT facilities.
- Ensuring effective operation of ICT facilities.

4.12 Do not send private, sensitive or confidential information either by email or to a public printer – particularly to an external recipient - if accidental disclosure could lead to significant harm or embarrassment. Anonymise personal data where possible, e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients if possible.

4.13 Websites should not be created on school equipment without the written permission of the Headteacher.

4.14 No one may use ICT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law, or may impact the image or reputation of the school.

4.15 The following content should not be created or accessed on ICT equipment at any time:

- Pornography and "top-shelf" adult content.
- Material that gratuitously displays images of violence, injury or death.
- Material that is likely to lead to the harassment of others.
- Material that promotes intolerance and discrimination because of race, sex, disability, sexual orientation, religion or age.
- Material relating to criminal activity.
- Material relating to any other unlawful activity e.g. breach of copyright.
- Material that may generate security risks and encourage computer misuse

4.16 It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headteacher. This may avoid problems later should monitoring systems be alerted to the content.

4.17 Users must not connect any personal ICT equipment (e.g. laptop, tablet) to the school network without the authorisation of the Headteacher and the ICT technician

4.18 All portable ICT equipment should be locked away or safely secured when not in use. Any staff authorised to use portable equipment, such as a laptop, for home must take all reasonable efforts to keep the equipment safe and secure. No cameras should be taken home, all pictures must be downloaded at school. Tablets can be taken home but only when given permission from the headteacher and only for specific classroom use ie update the "early learning goals". No personal photographs or personal apps must be downloaded. Learning Journeys must only be emailed to personal school email addresses.

4.19 For security purposes users should log off or lock their computer if they expect to be absent from their computer for any length of time. Users must shutdown their computer at the end of the day.

4.20 Digital recording equipment e.g. cameras may be available for staff to use as part of delivering ICT and the broader curriculum. Safe and appropriate use of recording equipment should be discussed with the children as part of the curriculum and referred to whenever recording is to take place.

4.21 Staff must not use images and recordings for activities and purposes beyond school endorsed projects. Staff should be aware of the students whose parents have expressly requested that photographs are not to be taken of them.

5 MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

5.1 Staff are advised not to give their home telephone number, mobile phone number, or personal email address to pupils.

5.2 Staff should only communicate electronically with children/pupils from school applications such as "I am Learning".

5.3 Staff should not enter into instant messaging communications with children or parents.

6 SOCIAL NETWORKING SITES

6.1 Staff should not connect with any current pupil on any social networking site.

6.2 Staff that use social networking sites should not discuss work-related issues and should not bring the school's reputation in to disrepute.

To be reviewed bi annually.