ICT Network & Equipment Terms of Use Policy

Review date: Feb 2018

Next review: Feb 2019

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

This policy and any Acceptable Use Agreements (for all staff, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Purpose

This policy is intended to ensure that all staff, pupils and visitors use the network and associated ICT resources in an appropriate manner and are aware of their duties and responsibilities by adhering to these guidelines.

Servers, network and access

Servers are kept in a locked and secure environment, password protected and screen locked.

Access rights are limited to ICT Support Staff.

Backup media is encrypted by appropriate software.

Back up tapes/discs are securely stored on-site and a copy kept off-site where appropriate.

Remote back ups are automatically securely encrypted.

Access

Users are responsible for all activity on school systems carried out under any access/account rights assigned.

No unauthorised person may use school ICT facilities and services.

Users should keep the screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.

Users should lock their screen before moving away from a computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

Users should ensure that they log off from the PC completely when away from the computer for a longer period of time.

It is imperative that users do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.

Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

Hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read.

Passwords and Password Security

Every member of staff is issued with an individual network, email and Management Information System (where appropriate) log-in username and password.

Changing a password will be required whenever there is any indication of possible system or password compromise.

Passwords or encryption keys must not be recorded on paper or in an unprotected file.

Passwords should only be disclosed to authorised ICT support staff if necessary, and never to anyone else.

Breaches of security with any password or account should be reported to the ICT support staff immediately who will action a password change, and to the Head teacher.

Passwords for staff who have left the School should be changed immediately/accounts disabled and accounts deleted from the system at the end of the appropriate school year.

Staff have an individual responsibility to protect the security and confidentiality of the school networks and MIS system**.** Individual staff users must also make sure that teacher workstations are not left unattended when logged on and logged off when not in use.

Remote file access:

Individuals are responsible for all activity via the remote access facility and should agree its use as follows:

Only equipment with an appropriate level of security should be used for remote access.

To prevent unauthorised access to school systems, all access information such as logon IDs and PINs must be kept confidential.

Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

Staff are issued with an encrypted memory stick for storing or transferring sensitive data outside of the school network.

Wireless Network

The school provides a wireless network for mobile devices for internet access and shared storage facilities in classrooms. This is managed by the ICT support team who configure each device individually.

Guest wireless access is available for staff personal use according to the agreed policy; Visitor access is also available once they have read and signed our visitors' agreement. **;** visitors' will be

issued with a temporary key for the duration of their visit eg governors meetings also according to the agreed policy; all activity must be in keeping with school policy use.

Monitoring

All users are made aware that internet and email activity is logged by the school's internet provider and agree to use it under those conditions.

e-Mail

The use of e-mail within most schools is an essential means of communication. In the context of school, e-mail should not be considered private.

Managing e-Mail

The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

Staff sending e-mails to parents are advised to cc. the deputy head using the account deputyhead@ashley.surrey.sch.uk.

Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

The forwarding of chain letters is not permitted in school.

All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.

Staff must inform the deputy head if they receive an offensive e-mail.

However a user accesses school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

School e-mail should be checked regularly by all staff.

Users should not use the e-mail systems to store attachments. It should be saved to the appropriate shared drive/folder where it will be backed up.

The automatic forwarding and deletion of e-mails is not permitted.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

Staff are not permitted to access their personal social media accounts on school equipment.

Staff must ensure that their personal use of social media does not in any way create a potential conflict with their professional status.

Pupils are not permitted to access their personal social media accounts whilst at school.

Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

Staff, governors, pupils, parents and carers are made aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

Staff, governors, pupils, parents and carers are made aware that their online behaviour should at all times be compatible with UK law.

Portable & Mobile ICT Equipment & Removable Media

School Devices

Mobile ICT devices provided by the school are configured and managed by the ICT Support Staff and no attempt should be made to alter this configuration in any way. Unauthorised access or unauthorised modifications to computer equipment, programs, files or data is an offence under the Computer Misuse Act 1990.

School cameras are provided for use by each class, the Office Staff, Sendco and SNAs.

The ICT Support Staff will log all ICT and camera equipment and its associated asset tag as part of the asset register.

The installation of any applications or software packages must be only carried out by ICT Support Staff, who will ensure licence compliance and data security.

Portable and mobile ICT equipment must be made available to ICT Support Staff when requested for software installations and updates, patches or upgrades.

All redundant mobile ICT equipment will be disposed of in accordance with Waste Electrical and Electronic Equipment (WEE) directive and Data Protection Act (DPA).

Their Use

Mobile devices are provided by the school for staff and pupil use within the school and must be used under the terms of the appropriate Acceptable Use Policy at all times. Pupils should only use when them when in a supervised environment.

In areas or situations where there are likely to be parents or members of the general public may be in the vicinity, portable or mobile ICT equipment should be locked with a security cable or kept in a locked cabinet, cupboard or room.

Staff using mobile devices for administrative purposes must ensure that all work is stored on their school network area where it will be regularly backed up; it should only be saved additionally on the mobile device/ laptop if the drive is encrypted.

No mobile devices may be used outside school except cameras. The exceptions currently are

- Laptops/tablets issued to Senior Management Staff, on the understanding that they are considered to be covered by the individual's insurance policy when doing so and are not used by any other party under any circumstances.
- Netbooks configured for offsite use on school trips/business (by prior arrangement with ICT Support Staff).
- Teacher tablets for assessment purposes and record keeping.

School data including photos should not be stored on the local drives of any portable device except on a very temporary basis eg downloaded to the storage area later the same day.

Removable media owned by the school may not be used to store or transport any confidential school data or data which may identify individuals or contain photos or video of pupils. The only current

exception to this is the encrypted drive provided by the school for website updates.

Images of children should only be taken and stored in compliance with the current school policy.

Personal Devices including Removable Media

Privately owned ICT equipment may not be connected to the school network, only equipment owned by the school is permitted such access.

Staff use of personal mobile devices during their working school day should be limited, discreet and appropriate e.g. Never in the presence of pupils or parents.

Mobile devices should be left in a safe place during lesson times. The school cannot take any responsibility for items that are lost, damaged or stolen.

Personal devices or digital media may not be used to store or transport any confidential school data or data which may identify individuals or contain photos or video of pupils.

Staff should never contact pupils or parents from any personal mobile device account or give their personal contacts to pupils or parents.

Staff should never send any emails, texts or images from their personal device that could be viewed as inappropriate to their professional role.

Staff should never use their personal device to photograph/video or store such images of pupils, or allow themselves to be photographed by a pupil(s). This guidance should be seen as a safeguard for members of staff and the school. (See 'Use of Images' Policy).

Staff should understand that failure to comply with the policy is likely to result in disciplinary procedure.

No pupil is permitted to bring to school any personal mobile device including a digital camera with the exception of one mobile phone in year 6 which must be given to the teacher at the beginning of the school day and will be returned at going home time. These must be used within the terms of the pupil agreement. Digital cameras may be used at pupils' own risk on trips (day and residential); it is the child's responsibility to look after their own equipment. (See 'Use of Images' Policy).

Review Procedure

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.