Staff Computer Policy

Introduction

The purpose of this policy is to provide guidance to staff on the operating of the school computer network and what is deemed acceptable practice. This policy runs in parallel with the staff social media policy. All staff must indicate that they have read and understood this policy. The Head of Education/ICT Co-ordinator will clarify any areas upon request.

Computer equipment is defined as:

a) that which is the property of the School or leased/rented to it; or

b) on loan to the school from third parties; or

c) used on the school premises, irrespective of ownership and 'computing and/or network resources'

The school network includes all communication equipment that transmits information electronically. For the avoidance of doubt this includes all smart phones and tablets and any new devices that may be developed that are capable of connecting to the school network.

Safeguarding/Security of Computer Information

All persons responsible for computer equipment of any type must take adequate precautions to ensure that the physical environment is secure in order to prevent illegal access to equipment and/or theft. The level of physical security should be appropriate to the type and location of the equipment.

In all instances where sensitive data of any kind are held, irrespective of whether or not data protection legislation applies, every effort must be taken to ensure that the data is secure. In this context data includes passwords and other levels of access security, and the threat to secure data includes possible introduction of viruses. All sensitive data on any mobile devices (including laptops, USB pen drives, removable media) must be secured or encrypted. Strong passwords must be used which must not be shared with other users.

All important data must be backed up regularly to guard against media or mechanical failure. A suitable backup strategy and implementation must be adopted appropriate to the type and location of the equipment.

All computer procedures and data are subject to review by the School's internal and external review.

General conditions relating to use of specific systems

Every person who connects to and uses computing and/or network resources owned or controlled by the School shall abide by the conditions of use including but not exhaustive of the ICT Policy and Social Media policy.

Persons connecting to and using computing and/or network resources external to the School must abide by any conditions of use and satisfy any registration conditions imposed by the external agency.

General disciplinary offences

A breach of any provision of these conditions of use shall itself constitute a disciplinary offence.

Non-compliance with the Computer Misuse Act 1990 constitutes a disciplinary offence.

Any person who wilfully and knowingly gains unauthorised access to a computer system commits a disciplinary offence.

Any person who wilfully, knowingly and without authorisation attempts to introduce a virus or other harmful or nuisance program or file, or to modify or destroy data, program or supporting documentation residing or existing internal or external to a computer system or computer network commits a disciplinary offence.

Staff must not download any unauthorised software from any source.

Illegal or unlicensed audio and video files must not be downloaded from the internet or any other source.

Any person who changes any software policy settings on any School computer without prior permission from the ICT Curriculum Manager may have their computer rights revoked and may face disciplinary action.

Contravention of any of the policy statements in this document shall constitute a disciplinary offence, and may, depending on the severity, amount to gross misconduct.

Offensive and indecent material and messages

Non-compliance with the Obscene Publications Act 1959 constitutes a disciplinary offence.

Any person who:

a) creates, displays, produces, circulates or stores by means of a computer, computer system or computer network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character, commits a disciplinary offence.

b) creates, displays, produces, circulates, or stores by those means, for the purpose of causing annoyance, inconvenience or needless anxiety to another, a malicious message, including email, commits a disciplinary offence.

Network management and network security

Any unauthorised person who attempts to monitor traffic on the School network commits a disciplinary offence. Any person who enters any restricted area without authorisation commits a disciplinary offence. For the purposes of this condition, restricted area includes all ducting and other containment carrying network equipment or cables.

Personal equipment may not be connected to the school computer network without the authorisation of the Principal.

Wilful damage

Any person who by any wilful or by deliberate act jeopardises the physical integrity of any computing and/or network resource, computer equipment associated environment conditioning equipment or physical network or power connections or associated accommodation commits a disciplinary offence.

All School file servers and workstations have up-to-date anti-virus software installed to help with the prevention of accidental loss of data. This software is kept up to date by the ICT Curriculum Manager.

Further action

The School reserves the right to:

a) deny all further access to relevant computer, computer system or computer networks for a defined period of time.

b) recover all reasonable costs howsoever incurred in investigating and subsequent restitution of computer, computer systems and computer networks resulting from any actions previously listed.

c) refer any possible criminal action to the police

OTHER MATTERS

School liability

The attention of users is drawn to the fact that the School will not accept claims made by third parties arising out of the application and use of results obtained from School computing facilities. The School accepts no responsibility for the loss of any data or software or the failure of any security or privacy mechanism.

Registration and use

All use of computing and/or network resources shall be made on the understanding that the use is solely for School purposes, and solely for the authorised user who is allocated the resource.

Where registered users are allocated a computer identifier (user name/password), they must use all reasonable endeavour to ensure that its integrity is maintained. This will include strict compliance with School rules relating to the regular changing of passwords Registered users must report any suspected breach of such security to the ICT curriculum manager.

Equipment

No computer equipment or associated facilities may be removed from their location without authorisation. Authorisation must be obtained from the ICT Curriculum Manager. Users are responsible for and must take reasonable care of any facilities loaned to them and may be required to pay the value of any facility damaged or not returned.

Data Protection Act 1998 (To be superseded by GDPR commencing May 25th 2018)

Every person shall comply with the requirements of the Data Protection Act 1984 concerning personal data. The Act enunciates eight principles relating to the collection, keeping and disclosure of personal data.

1) Data must be processed fairly and lawfully;
2) Personal data can be obtained only for specified purposes;
3) Personal data should be adequate and relevant and not excessive;
4) Personal data must be accurate and up to date;
5) Information should not be kept for longer than is necessary;
6) Data must be processed in accordance with the rights of the subjects;
7) Appropriate technological measures must be taken;
8) Personal data cannot be transferred to countries outside the EU unless the country provides an adequate level of protection.

**** This policy will be reviewed in conjunction with the EU's General Data Protection Regulation (GDPR) which will replace the existing DPA in May 2018.*

Software registration and prevention of piracy.

Licences concerning hardware and software must be registered and where appropriate signed by an authorised signatory. All persons who are licensed to use software or who control access to any computing and/or networking resource are obliged to take all reasonable care to prevent illicit use of software and documentation.

Internet access (to operate in conjunction with the staff social media policy).

A managed firewall system operated by third parties is in place to improve the security of the internal infrastructure of the School's computer networks.

Internet filtering software is installed ensuring that unwanted web sites and e-mails can be blocked.

The School records and monitors all internet access for all users. Users must not visit sites that could be deemed inappropriate or bring the school into disrepute.
Sensitive data must not be sent via e-mail unless it has been encrypted.

Defamation Act 1996

Complaints regarding defamatory material on the School networks and websites must be reported to a member of the Senior Leadership Team.

Any material which the School has been informed is defamatory will be removed or denied access by the ICT Curriculum Manager

Copyright

Users must abide by copyright law. Any suspected breach must be reported to a member of the Senior Leadership Team.

Source: Personnel	Date: Jan 2018	Review: Jan 2020