subrideo
moving business forward

Curriculum Acceptable Use Policy

July 2014/ Reviewed June 2015

It is the responsibility of the school to ensure all staff curriculum network users sign, print and date this document, then return it to the school administration team. The school is responsible for retaining such information for the purpose of audit reviews.

The purpose of this Policy is to describe the procedures and processes in place to ensure the safe and secure use of the School's curriculum network, its users, and to protect School systems and data from unauthorised access or disclosure.

This Policy document has been provided by the schools IT Support Representative; Subrideo. This Policy document refers to the school curriculum network only, and users operating within its confinements. This document does in no way associate itself with the school admin network. The school admin network is governed by the local authority.

Any queries arising from this Policy or its implementation, can be taken up directly with the school head teacher, or IT Support Representative: info@subrideo.co.uk

Summary of Contents:

1. Scope

i. This policy is intended to be read by all staff for general information and awareness, and makes reference to more detailed information and guidance in additional specific Policies.

ii. The policy is relevant to all Information and Communications Technology (ICT) services irrespective of the equipment or facility in use and applies to:

iii. All employees and others using the School's equipment and facilities.

iv. All use of ICT throughout the School.

v. In addition, all Users of ICT and other School facilities are reminded that there are elements of the curriculum network Acceptable Use Policy (AUP) which also apply.

vi. The Policy also takes into account the creation, management, processing and sharing of information. Therefore, this is an information security policy which incorporates use of ICT (hardware and software), electronic communication (Email, telephone and fax) and issues relating to the storage and use of data, including confidential information.

vii. The use of E-mail using Microsoft Office 365 or Google Apps for Education are the subject of a separate policy.

2. Introduction

i. The School has a large investment in the use of ICT which is used to the benefit of all groups and service users.

ii. In many areas of work the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of all ICT systems and data are maintained at a level which is appropriate for the School's needs.

3. Policy Objectives

i. The policy has three main objectives, to ensure that all of the School's assets; staff, pupil's equipment and data are adequately protected against any action that could adversely affect the ICT services required to conduct the School's business, and the accuracy and confidentiality of information held.

ii. To ensure that all staff are aware of and fully comply with all relevant legislation.

iii. To create and maintain within all groups and departments a level of awareness of the need for ICT and information security to be an integral part of day to day operations and the responsibility of all staff to comply with this and other relevant policies.

4. Responsibilities

i. All users of ICT systems are required to formally acknowledge receipt of the ICT Security Policy and that they have read and understood its content.

ii. All users of ICT systems are required to formally acknowledge receipt of the network acceptable use policy and that they have read and understood its content.

iii. ICT and information security is the responsibility of the School as a whole and consequently a responsibility of all members of staff and other authorised users. The policy has been approved and adopted by the Chief Executive.

iv. All providers and users of ICT services must ensure the security, integrity, confidentiality and availability of all data they create, process or use.

5. Violations

i. ICT and information security is viewed seriously by the School and any breach of this policy could lead to appropriate action being taken against those who commit such a breach. Violations will be addressed under appropriate procedures and may include the Disciplinary Procedure.

ii. Violations of this Policy will include, but are not limited to, any act which:

iii. Exposes the School to actual or potential monetary loss through the compromise of ICT security;

iv. Involves the creation, processing or use of any data found to be inaccurate or invalid;

v. Involves the accessing, creation, processing or use of any data by unauthorised users;

vi. Involves the disclosure of confidential and/or personal information, the unauthorised use of corporate data and/or the sending of defamatory information;

vii. Involves the creation, use, downloading or transmitting of any data or other material for illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement or government body.

viii. Involves unauthorised modification, installation or use of software, or the modification, installation or use of unauthorised software

ix. Any individual who has knowledge of a violation of this ICT & Information Security Policy must report that violation immediately to the school head teacher or school governing body.

6. Network Access

i. Access to the network, and any equipment, application, database or other resource must be by individual login – i.e. unique user name and password. Other than in very exceptional circumstances, generic login credentials are not permissible.

ii. The school provides computer equipment such as laptops for business use, which are built for compatibility with the School's network and internet connection. School equipment must not be connected to other networks or internet services.

iii. Non-School computing equipment must not be used to access School network resources unless authorised by Information Services.

iv. All external use of the network must be by named individuals only, authorised by an appropriate manager. Access will only be permitted by a network, and will be by unique user name and password.

v. The creation of new accounts is carried out by the network administrator, on request by the school intranet 'new, delete, amend user' form, detailing the appropriate access levels and permissions by the school administrative team. Whenever possible the new user form must be submitted not less than 1 weeks prior to the new employee starting work. Temporary staff must have a leaving date stipulated within the request form, this allows an expiration to be set on the account. The request for a print account code (where/when required), must be stipulated from the school intranet 'new, delete, amend user' form.

vi. The deletion of old accounts is carried out by the network administrator, on request by the school intranet 'new, delete, amend user' form. Whenever possible the delete user request must be submitted not less than 1 weeks prior to the new employee starting work.

vii. All users must only access, or attempt to access, what is permitted by their profile. If there is any difficulty in accessing files or programmes, the user must create a fault ticket using the school intranet electronic fault log. Alternatively, the user must inform a member of the school administrative team, who in turn must log the fault ticket.

viii. If access to a file held in an individual's K: Drive is necessary and that person is not available, e.g. they are off work sick, then the line manager must contact IT network administrator for assistance. The reason for the access, the full name of the file and the identity of the person holding it will be needed.

ix. As a principle all users must retain their files on their K: Drive.

x. Data stored on a computer's hard drive is not automatically backed up, and may be accessible to anyone switching on the PC. A computer hard drive is therefore not secure and must be seen as a last resort and a temporary, short term solution. Similarly, data must not be stored on non-School equipment.

xi. Where a computer is shared by a number of users, it is essential for all users to log off the computer before leaving it. A user is responsible for all work carried out on a computer using their login details, including internet access and email use, whether or not that user was actually using the computer themselves.

xii. The network will require a password change every 90 days. Any accounts with no activity during a 90 day period will be disabled. A further 90 day period of inactivity will result in the account being deleted. An appropriate manager will be informed, and an offline backup copy of any data will be created.

7. Segregation of Duties

i. Access to systems and applications is restricted according to the role and business requirements of each user. Access rights are established and managed on a need-to-know basis, and agreed by a user's line manager and the owner of the system or application.

ii. In general, access rights comprise the functions of read, write, delete and execute and these are allocated to each user in respect of each system and application. Full control is never granted to network shared folders, with the exception of that user's home folder (K: Drive). Unique user ID's are assigned to all individual user home folders (K: Drives). Group ID's (Security Groups), are split into the following groups; Staff Security Group and Pupil Security Group.

iii. Access rights must be reviewed once every quarter, to ensure that access to systems and applications remains appropriate and consistent. A review should also take place after any changes to the system, such as a system migration.

iv. On receipt of a "Delete User" instruction, access rights to all systems and applications associated with that user must be revoked immediately.

v. System Administrator access allows full unrestricted rights to defined systems and applications for management purposes, including the creation and removal of system users. This level of access must be kept to the minimum number of individuals required to enable day-to-day operation and emergency access in the event of a system failure. System Administrator access should be via unique individual ID.

vi. The use of privileges in systems and applications must be allocated in a restricted and controlled manner. Privileges enable users to override some controls within a system, usually for system management purposes, and privileges must be removed when no longer required.

vii. Access to systems and applications by third parties, such as software maintenance/ support personnel, must be subject to prior review by the school head teacher and governing body. Access by third parties must be restricted to only those systems, or parts of those systems, that are required and must be revoked as soon as it is no longer required.

8. Passwords

i. Passwords must be used in order to access computers, applications, systems and all other networked resources

ii. Passwords of staff members must meet complexity requirements; alpha-numeric, contain eight or more characters of which at least one must be a digit. Passwords of pupils must be 4-digit randomised numeric passwords.

iii. Passwords must not be proper names, address names or birth dates. Network login / user names must not be used in any form (reversed, capitalised, or doubled as a password).

iv. The same password must not be used for more than one application, system, device or service.

v. Network passwords cannot be re-used within 24 password changes

vi. The network will prompt for a password change every 90 days. However, for additional security, Users should consider changing their password more frequently (preferably every 30 – 40 days) both for network access and for specific systems.

vii. If a software package comes installed with a default password, that password must be changed immediately after installation.

viii. Passwords must not be posted in a location accessible by others (such as a note stuck to the monitor, under the keyboard or even in a desk drawer).

ix. Passwords must NEVER be divulged to or shared with anyone else. If a user is asked for their password over the telephone by someone purporting to be from Information Services or any outside authority, company or organisation, it must not be given.

x. A machine must not be left unattended while logged onto a system unless the password protected screen saver has been activated or the computer has been locked. Automatic password-protected screensavers are applied across the network, following a period of inactivity of 20 minutes.

xi. Where files or data need to be shared between individuals the data must be held in a networked, restricted shared folder.

xii. Users must remember that they are at all times responsible for anything undertaken with their user id and password.

xiii. If a user requires a password reset, the user must liaise with a member of the school administrative team or ICT coordinator. It is required that the administration team member or ICT coordinator completes and password reset request using the school intranet 'new, delete, amend user' form. Printed versions of all user account password resets are handed to the end users in sealed envelopes. The end user will be required to reset the pass word upon next logon.

9. Physical Security

i. All hardware devices must bear an asset tag sticker, which must not be removed throughout the life of the device.

ii. All desktop devices, e.g. PC, printer and scanner, must have adequate precautions taken to protect them against theft and accidental damage in addition to environmental threats and hazards. All manufacturer and supplier instructions and advice must be followed.

iii. Security precautions should, in the first instance, concentrate on adequate building security and siting of the device in the office, and then may extend to simple lock down devices attached to a desk.

iv. All ICT hardware purchasing must be coordinated the school IT support representative (Subrideo). This ensures that equipment in use across the School is consistent, meets appropriate standards and is compatible with existing equipment and network resources.

v. All desktop computer equipment should be turned off when not being used for an extended period of time.

vi. Equipment will be protected centrally by an Uninterruptible Power Supply (UPS) and where necessary controls must be in place to ensure a clean power supply by eliminating the impact of power spikes.

vii. Server rooms, data centres and all other secure or sensitive areas must be subject to additional security measures including controlled and authenticated access.

viii. It is recommended that all such areas should also be made secure. All buildings should be alarmed and/or security grilles should be in place where appropriate

ix. See the Physical Entry Controls and Secure Areas Policy for more information.

10. Portable devices /Removable Media

Including: USB Pens, External USB Hard Drives, Memory Cards.

i. When not in use all portable devices such as laptop computers must be retained in a secure environment. This may include a lockable store cupboard with controlled access, or lockable metal cabinets, but again with controlled access.

ii. All portable devices must be security marked (etched, UV pen, etc.) as soon as received into a department or service, and then added to the appropriate inventory.

iii. When portable devices are taken off premises, all users must ensure that they take adequate precautions to protect the equipment against theft or accidental damage at all times, e.g. not left visible but locked away.

iv. No portable devices must be left in an unattended vehicle at any time.

v. All School laptops leaving site, must be encrypted to ensure safe guarding of data.

vi. The School must make users aware of insurance arrangements and the user's obligations before allowing the device to be taken off the premises.

vii. Users who travel with School laptops must make regular backups of data contained on the laptop.

viii. Laptop computers must not be connected to the network unless anti-virus software has been installed. It is the user's responsibility to ensure the anti-virus software is kept up to date, a fault ticket must be logged by the user, in the event of an issue with the anti-virus software updating.

ix. Records must be maintained by the school administrative team, which detail their portable devices including type, serial number. A record for signing out and return of the device must be put in place.

x. Portable devices must only be used in connection with the School. Portable devices such as USB storage pens, hard drives and memory cards must be encrypted. Only encrypted devices are sanction for use with School.

xi. Portable devices must never contain any more data than is the absolute minimum required.

11. Software Installation

i. Only software for which the School is licensed may be installed upon any School computer. Network security prevents users from installing software. Software installations can only be carried out by a network administrator.

ii. Appropriate action will be taken against any user found to have installed software that is not properly licensed or if the software is being used contrary to its license agreement.

12. Security Incidents

i. A Security Incident is a situation where the security of a PC, a system, an application or the network has been compromised, and may be from an internal or external source.

ii. Examples would include Users who have accessed data or material which their User Profile should have prevented them from seeing, or perhaps accessed a system or application at a user level to which they are not entitled. It could also be the introduction of a virus to a PC and / or the network, or network access by an unauthorised user.

iii. Any individual who becomes aware of a security incident must report it as soon as possible.

13. Security Weaknesses

i. A weakness is a situation whereby potential for a security incident is identified. A PC may be left unattended, logged into a system without a password-protected screensaver or other locking procedure potentially allowing access by unauthorised users.

ii. Further examples could be the inclusion of too many individuals in a system's Administrator profile or a lack of procedures for signing out laptops or other portable devices to individuals, potentially allowing unidentified and/or unauthorised use of the equipment.

iii. A weakness does not have to be specifically ICT-related. It could be windows left open close to portable equipment, or a PC monitor displaying potentially sensitive data positioned to face a window.

iv. Any individual who becomes aware of a security weakness must report it as soon as possible.

14. Security Breaches/ Violations

i. A security breach is an activity which causes or has the potential to cause the loss, damage or corruption of data. This may be the result of a specific Security Incident, a Security Weakness, a Violation of security policies or procedures or a combination of all three.

ii. A security violation is any activity which contravenes the ICT & Information Security Policy and other related policies, procedures and guidelines and may result in a security breach.

iii. Any individual who becomes aware of a security break or violation, must report it as soon as possible.

15. Virus Prevention and Control

i. A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus can also transmit itself across a network, spreading the infection to other computers and devices.

ii. The general term is "malware", which covers various types of virus, worms, Trojans, and spyware. A virus can cause performance problems or more long term damage to a computer or network.

iii. Malware is most commonly introduced to a computer through internet downloads and as attachments to emails.

iv. If a virus is found, or suspected, to be on a machine or external storage media, the user must inform a member of the network administrator or office administrative team. Users must also create a fault ticket on the School intranet electronic fault log.

v. On occasion the network administrator may inform users, through the School intranet announcements section, concerning a particular virus and its effect. All Users must take appropriate action when so notified. Deliberate contravention of such a notification is a potential disciplinary matter.

vi. No equipment capable of processing information, whether desktop or portable, must be implemented on the network without appropriate anti-virus software being installed.

vii. All software must be checked for viruses before installation on any School device, including computers, laptops and other portable devices.

viii. Where a USB memory stick or other storage media are used to transfer files, program or data, from one machine to another it must be virus checked before use, particularly if it is from an external source, a different department or service or from a stand-alone machine which may not be fully protected against viruses.

ix. If there is any doubt as to the origin of the files being transferred, they must always be checked for viruses before use.

x. All network devices are updated automatically via the School antivirus server, as a primary update location, with a secondary update location pointing to the antivirus developer's web servers. Users must always check to ensure their antivirus software is up-to-date and functioning correctly.

xi. As a matter of principle, files downloaded from the Internet must initially be saved onto the User's hard drive (C: drive) and virus checked before opening or executing. Only when it has been found to be clear of viruses can it then be transferred safely to other areas, such as shared folders and K: Drive folders.

xii. In the event of a user working with the Microsoft Outlook Client, antivirus is installed to monitor the sending and receiving of email.

16. Sending Confidential Information

i. It is the responsibility of all employees of the School to safeguard the security of confidential and/or personal data for which they are responsible, or which they access in order to carry out their job. There is also a responsibility to bring to a manager's attention any areas of concern regarding the transfer or transportation of such information.

ii. Before making information available to anyone else, employees must make sure that they have the authority to disclose it.

iii. Email is not a secure means of communication outside the security of the School's network and must not be used for sending personal or sensitive corporate data.

iv. Even when emailing within the security of the School network it is important to ensure the name and email address of the recipient is correct, and that a suitable subject line is used which does not include personal information.

v. The sender must also ensure that the recipient is expecting the information and confirm that it has been received successfully.

vi. Electronic data physically transported between sites, departments or organisations must be encrypted, properly packaged and clearly labelled to ensure it is handled correctly, and not corrupted by magnetic fields or other environmental damage.

17. Termination of Employment

i. When a user who has network access leaves the employment of the School the appropriate manager must arrange for the transfer of any necessary files and e-mail folders.

ii. Where termination is due to ongoing disciplinary action the user's access will be denied with immediate effect.

iii. On termination it is the user's responsibility to return all equipment, entry passes, software, documentation (both paper and electronic) and any other School asset in their possession.

18. Disposal IT Equipment and related Media

i. All PCs which have become obsolete or are surplus to requirement must have their hard disks checked for content. Software that is being transferred to another machine must be uninstalled and all data files must be deleted.

ii. The collection/disposal of all old/defective IT equipment is carried out by accredited disposal companies, of which comply with WEEE regulation standards. Users must not arrange individual disposal of School equipment

iii. All removable media must be rendered unusable before disposal. It should be noted that reformatting does not delete all data from disks and such data can subsequently be recovered using freeware.

iv. CD and DVD disks containing confidential and/or personal information must be re-formatted prior to disposal or re-use. Read-only CDs & DVDs must be rendered unreadable by shredding, scratching, heating or otherwise destroying the disk's surface. Other CD or DVD disks can be disposed of through the general waste disposal procedure.

v. All paper records can be disposed of through the School's general waste disposal procedure. However, paper documents containing confidential and/or personal information must first be shredded

6. Audit and Review

i. ICT and information security is managed through the IT support contractor, school head teacher, school ICT coordinator, school administrative team and school governing body. ICT and information security is subject to regular audit and review.

All staff users must read the aforementioned text, then complete the section below.

Accepted by	
Name:	
Signed	
Date	

It is the responsibility of the school to ensure all staff curriculum network users sign, print and date this document, then return it to the school administration team. The school is responsible for retaining such information for the purpose of audit reviews.