IT ACCEPTABLE USER (STAFF)

1. Introduction

1.1 The School's IT resources are essential to the effective delivery of educational provision. Computers and other networked facilities including Internet access are available to staff and pupils within the School and should be used to promote educational learning. It is therefore vital that all staff, agents and contractors are aware of the School's policies and procedures relating to the use of IT resources. A poorly administered network or weak password controls could expose the School's information to an unauthorized user or introduce a virus infection.

2. Scope

2.1 This policy applies to all School employees, contractors and agency staff who have access to the School's IT network and resources and are assigned School IT equipment including laptops. For the purpose of this policy ICT resources are defined as any computing device (fixed or removable) including servers, workstations, laptops etc that can be connected to the School network or receive data from the network

3. Responsibilities of School staff when using IT resources

3.1 To ensure that school IT resources are utilised effectively it is essential that all staff:-

- make careful and considerate use of the School's ICT resources, report faults and work in a way that minimizes the risk of introducing computer viruses to the system. Faults should be reported to the office and logged in the fault report book which is kept in the office.
- protect students in school from the harmful or inappropriate material accessible via the Internet or transportable on computer media;
- recognize their responsibility to maintain the privacy of individuals, comply with current legislation and the expectations of the School;
- know and abide by the School's Acceptable Use Policy as it applies to them and to the people in their care.

4. Laptops and encrypted memory sticks issued to staff

4.1 The laptop and encrypted memory stick remains the property of the School and is provided to users on a loaned basis. The laptop or encrypted memory stick provided must not be used by any person(s) other than the authorized user to whom it has been allocated and the property identification tag attached to each laptop should not be removed for any reason.

4.2 School laptops have a predetermined list of software installed on the hard drive. No addition or deletion of any software or hardware is permitted without the express permission of the Head Teacher or School IT Technician. To ensure that security patches and virus definitions are up to date staff should connect the laptop to the School network on a regular basis.

4.3 All reasonable care should be taken to prevent loss, damage, theft or unauthorized use of IT equipment as far as is practical. For example, the laptop or encrypted memory stick should never be left in a vehicle overnight or other unsecured, vulnerable situation. Any loss or damage to School IT equipment should be immediately reported to the Head Teacher or School Business Assistant.

4.4 When a contract of employment at the School ends, the employee must return all computer equipment and software to the School Business Assistant in full working condition. The user account and all personal work stored on the laptop and encrypted memory stick will then be securely deleted.

Policy approved……..at a Full Governors Meeting

Date of meeting: 24 October 2018 **Minute Number: 12.2** **Renewal Frequency:** Annual

IT ACCEPTABLE USER (STAFF)

4.5 If software/hardware problems arise, the laptop may need to be restored to original settings. Work files may be lost during the process, therefore it is the responsibility of all users to ensure that backups of all files are regularly made to an external device such as the School's networked server or encrypted memory stick.

4.6 Where there is evidence that the laptop has not been used in accordance with the above guidelines, a charge may be made for the replacement or repair of any School laptop and encrypted memory stick whilst on loan.

5. Health and Safety guidance on using IT equipment including laptops

5.1 In the interests of health and safety, staff are advised to adhere to the following recommendations for the safe use of personal laptops. Any health and safety concerns associated with the use of laptops should be discussed with the Head Teacher.

- Sit in a chair that provides good back support to avoid backache and position the laptop directly in front of the user to avoid twisting;
- Take regular breaks from the screen to reduce eyestrain.
- Avoid using the laptop on a low table or on the lap as both of these positions will increase strain on the neck and lower back.

6. Use of other School IT Equipment

6.1 Users who borrow equipment from the School must sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use. Any loss or damage to equipment on loan should be immediately reported to the Head Teacher or School Business Assistant in the first instance and any theft or criminal damage should be reported to the Police.

6.2 To prevent data loss and ensure consistent application of School policies no personally owned equipment should be attached to the School's network without the permission of the Head Teacher. All mobile devices must be encrypted or password protected wherever technology allows.

7. Software

7.1 Users should use software in accordance with applicable licence agreements. To copy software or any supporting documentation protected by copyright is a criminal offence. The use, or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the School. Under no circumstances should any user possess unlicensed software on School premises or use unlicensed software on School IT equipment (including portable equipment).

8. Network Access, Passwords and Data Security

8.1 Users must only access information held on the School's computer systems if properly authorized to do so and the information is needed to carry out their work. Under no circumstances should personal or other confidential information held on the School network or IT equipment be disclosed to unauthorized persons. If you accidentally access information which you are not entitled to view report this immediately to the Headteacher or School Business Assistant.

8.2 Staff using computers in classrooms must ensure that sensitive data is not accessible to students or other individuals by logging off or locking the computer as appropriate. In other areas, computers must not be left logged on when left unattended. Alternatively where this is not practical all sensitive data must be password protected.

8.3 Staff passwords must be changed on a regular basis, at least termly. System and administration level passwords should also be changed on a termly basis at least.

8.4 All passwords are to be treated as sensitive, confidential information. Therefore, staff must not:

- Use School user account passwords for other types of access (e.g., personal ISP accounts, Internet banking, etc.).
- Share passwords with anyone, including colleagues, administrative assistants or IT Technicians.
- reveal a password over the phone or in an e-mail message or other correspondence.
- talk about a password in front of others including family members.
- hint at the format of a password (e.g., "my family name").
- reveal a password on questionnaires or security forms.
- insert passwords into e-mail messages or other forms of electronic communication.

8.5 If an account is suspected to have been compromised, the incident must be reported immediately to the Head Teacher or School Business Assistant so that the account password can be changed.

9. Encryption

9.1 Sensitive or confidential information should not be permanently stored on laptops or other portable devices e.g. memory sticks. Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done using the encrypted memory stick provided by the School.

10. Use of the Internet and E-mail

10.1 Internet and E-mail use is integral to the effective delivery of educational services provided by the School. Nothing in this policy should be read as restricting the proper use of E-mail and the Internet for School activities. Limited personal use of School's Internet and E-mail system is permitted subject to these principles and guidance notes.

10.2 Personal use of the Internet and E-mail system is permitted outside your normal working hours (i.e. before or after work and during your lunchtime). Occasional use of the E-mail system within working hours is permitted to respond to an urgent E-mail. Any personal use must not, in any way, distract staff from the effective performance of their duties. Improper or inappropriate personal use of the School's Internet and E-mail systems may result in disciplinary action.

10.3 Whilst personal use of the Internet and E-mail is permitted during lunch breaks and outside of working hours, staff should be aware that the Internet facilities are provided by the School. Any Internet activity and E-mails received/sent through the School's network personal or otherwise, are recorded and will be monitored.

10.4 Instant Messaging (IM) is a form of real time communication between two or more people based on typed text. You should not engage in 'recreational' chatting during working time that results in lost productivity or distracts other employees from their work. IM must never be used for the passing of personal information of any kind.

10.5 Many Internet sites that contain unacceptable content are blocked automatically by the School's filtering systems. However, it is not possible to block all "unacceptable" sites electronically in all circumstances. If you become aware of any sites which require re-categorization you should inform the School's Business Assistant as soon as possible.

10.6 Downloading of video, music files, games, software files and other computer programs - for non-work related purposes - is not allowed. These types of files consume large quantities of storage space on the system and may violate copyright laws.

10.7 Any personal or potentially personal information sent via e-mail or the internet is covered by the Data Protection Act 1998. In addition, e-mails may be covered by the Freedom of Information Act and may be disclosed as part

of legal proceedings. Employees should exercise the same caution when writing e-mails as they would in more formal correspondence.

10.8 Improper statements in an e-mail can give rise to personal liability and liability for the School and may constitute a serious disciplinary matter. E-mails that embarrass, misrepresent or convey an unjust or unfavourable impression of the School or its business affairs, employees, suppliers, students and their families are not permitted.

10.9 Extreme care must be taken when using the School's E-mail facilities to transmit information. Confidential or sensitive information should not be sent via the Internet or E-mail unless the data is fully encrypted using secure E-mail facilities.

10.10 Users must not form contracts or vary contractual terms over the Internet unless authorized to do so. Use of the Internet to buy goods or services for personal use will not render the School liable for default of payment or for the security of personal information disclosed.

10.11 Employees must not deliberately view, copy or circulate any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material, the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains images, cartoons or jokes that could cause offence
- appears to be a chain letter
- could constitute bullying

10.12 Where an employee receives an e-mail or accidentally accesses Internet sites which may infringe these guidelines, the Head Teacher must be informed immediately (whether for professional or personal use). The Head Teacher will then use her professional discretion whether to report the matter further. In this situation the member of staff concerned should ensure that a short written record is kept to clarify the circumstances.

10.13 Copyright law applies to many aspects of Internet use. Users must ensure that the School either owns the copyright, or has written permission from the copyright holder, for any material that they intend to upload, or cause to be uploaded, to the Internet, passed on by E-mail or transmitted to any third party by whatever means. When downloading material the School must observe any copyright statements that appear and, in the absence of any copyright statements, follow the normal practice as applied to printed materials. Unless otherwise stated on the site, all downloaded material must be for curricular or research use and must not be passed on to third parties. Many sites are now classifying their resources with a cc (creative commons) licence, enabling more appropriate use of the resource without the need to contact the copyright holder for permission.

11. Social Networking Sites, Internet Newsgroups, Blogging and Chat Rooms

11.1 You must not participate in discussions that may bring the School into disrepute and you must not give advice or information that you know to be contrary to the School's policies or interests. You should not engage in chat which embarrass, misrepresent or convey an unjust or unfavourable impression of the School or its business affairs, employees, suppliers, pupils or their families. **Remember that these sites are public forums.**

11.2 Use common sense when posting items. Think about the intended audience and the consequences of making unwise remarks about colleagues or the School. You must not reveal sensitive or confidential information relating to the School on any social networking sites.

IT ACCEPTABLE USER (STAFF)

12. Monitoring of Internet and E-mail Use

12.1 The School's E-mail system automatically records details of all E-mails sent both internally and externally including the name of the person sending and receiving the E-mail, contents of the message and details of any file attachments. In the event of suspected misuse or as part of standard monitoring procedures E-mails may be accessed to establish the content of individual transmissions and ensure compliance with current legislation.

12.2 The School will record the details of all Internet traffic. This is to protect the School and its staff from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited. Internet access logs will include the network identifier (username), address of the Internet site being accessed and the name of any file accessed and/or downloaded. All Monitoring information will be kept securely for six months.

13. Private Use

13.1 IT resources and facilities (including laptops provided to employees) are provided for School business purposes. Reasonable and responsible personal use is allowed, provided there is no conflict with the interests or requirements of the School. The School does not accept liability for any personal loss or damage incurred through using the resources and facilities for private use. The security of private information and data is the responsibility of the user.

13.2 In order to comply with the HM Revenue & Customs regulations on taxable benefits any use of a School laptop for an employee's private purposes must not be 'significant'.

14. Disciplinary and Related Action

14.1 Suspected misuse of the School's computer systems by a member of staff will be considered by the Head Teacher. Failure to follow the IT Acceptable Use Policy could result in disciplinary action being taken and include a warning, suspension, dismissal from the School and in the case of illegal activities referral to the Police.