Ken Stimpson Community School

IT Acceptable Usage Policy

Last Reviewed:- March 2018

Policy Cover Sheet

Document Name:	IT Acceptable Usage Policy
Type of document:	Policy
Purpose of document:	This document outlines the IT Acceptable Usage policy adhered to by Ken Stimpson Community School.
Intended audience:	Students, Staff and Parents
Document lead/author	Technical Services Manager

Contents

1. Introduction

- The purpose of this document is to ensure that all users (including but not limited to Employee, Students, Visitors, Contractors) of Ken Stimpson Community School (referred to as 'the School') computing facilities are aware of School policies relating to their use.

- The School encourages the use of computing (and other technologies, referred to as 'ICT Facilities') for the benefit of its users. The computing resources are provided to facilitate a person's work as a user of the School, specifically for educational, training, administrative or research purposes. The regulations that constitute this policy seek to provide for the mutual protection of the School and the rights of its users.

- Effective and proper use of information technology is fundamental to the successful and efficient running of the School. However, misuse of information technology – in particular misuse of e-mail, internet and social media – exposes the School to liability and is a drain on time and money.

- It is the responsibility of all users of the School ICT facilities to be aware of, and follow School ICT polices and guidelines and to seek advice in case of doubt.

2. ICT Facilities

- Access to ICT facilities are managed by IT Services. Use of ICT facilities is at the discretion of the Technical Services Manager and the School Senior Management Team (referred to as 'SMT')

2.1 Definitions

- The phrase 'ICT Facilities' as used in School policies are interpreted as including any computer hardware, printers, telephones, tablets, or software owned or operated by the School, including any allocation of memory/disk space on any of the School Systems & Cloud systems managed by the school

2.2 Ownership

- ICT facilities owned by the School and software and/or data developed or created (For whatever reason) on that equipment remains in all respects property of the School. The Patents Act 1977 and Copyright, Design and Patents Act 1998 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer

2.3 End User Devices

- End User Devices refers to all school owned: Desktop & Laptop Computers/Tablet/Mobile phones/Printers/MFDs & Cameras (Including video)

- End User Devices are a critical asset to the School and must be managed carefully to maintain security, data integrity, efficiency, reliability & compliance with other school policies. All end user devices purchased by the school & used within school under any department fall under the remit of IT Services in order to ensure this is carried out

- IT Services has measures in place to prevent installation of software, users must consult IT before purchasing any software for installation on the ICT Facilities. Attempting to bypass this restriction may result in access being revoked.

- Laptop & Mobile devices are at a high risk from loss or theft & require additional security protection. All reasonable precautions must be taken to ensure the hardware is stored securely.

- Maintenance or repairs not to be attempted by anyone who is not a member of the IT Services team. Any damage that occurs if an unauthorised user attempts to do so will be the responsibility of the person

- Access to unencrypted removal media (i.e USB Sticks/DVD/Memory Cards & Cameras) is restricted to IT services & encrypted removal media to authorised users only. Temporarily read only access may be granted on a case by case basis by contact IT support (i.e Visitors)

- In the event of a loss or theft of a device you should report the matter promptly to IT Services.

- All Photos, Videos & Audio captured via end user devices must comply with the schools recording policy

- End user devices are not to be taken off site without express permission of the Technical Services manager and/or the Principal.

- MFDs are provided for school business use only & should not be used for private printing.

- Colour printing is restricted to users who have a business reason for being able to print in colour. Access can be requested via SMT

- All end user equipment will be equipped with an Asset Tag & appropriate details recorded by IT Services. You must not attempt to remove this.

2.4 Loan equipment

- The policy regarding loan equipment is similar to that for laptops and mobile devices. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment will

be required to sign for it (or obtain a parental signature) and bear the responsivity of its care. Loan equipment should be stored securely when not in use.

- If loan equipment is stolen or lost you must report the matter promptly to IT services

- If damage occurs to loan equipment, please inform IT services – You should not attempt to fix or have the device repaired yourself.

- Confidential data must not be stored on any loan equipment, unless the device is encrypted & access is restricted & recorded accordingly.

2.5 ICT Disposal

- All ICT Equipment owned by the school must be disposed of by IT services using a WEEE certificated disposal company. All disposal documentation shall be kept within IT Services.

2.6 Software

- IT Services has measures in place to prevent installation of software by non IT Services staff. Attempting to bypass this restriction will result in deactivation of your IT account.

- Only software properly purchased and/or approved by IT services may be used on School hardware. Unauthorised software can cause problems with the stability of School ICT Facilities or run the risk of violating software licensing & copyright laws.

2.7 Network Access

- In order to use the ICT facilities of the School a person must first be provided with their own user name by IT Services. Registration to use the computer facilities implies, and is conditional upon acceptance of this Acceptable Use Policy. All staff & student users must have contact details & photo registered on the schools MIS (Management Information System) in order for access to be granted.

- Visitors to the school may have restricted access granted appropriate to their role via temporary login's, provided details are kept of users in question. Access is conditional of acceptance of this Acceptable Use Policy.

- Temporary staff (i.e cover teachers) may have temporary access granted via dedicated "cover" accounts. These are issued by the cover manager & terminate upon end of temporary employment. Access is conditional of acceptance of this Acceptable Use Policy.

- All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. Passwords protect the School's systems from access by unauthorised people; they protect your work and the School's information. The user is personally responsible and accountable for all activities carried out under their username.

- All users have access to appropriate shared areas on the School's file servers for the secure storage of files.

- Users will not store data unrelated to school business on the school ICT facilities, such as personal photographs, files or financial information. Users should expect no privacy with regards to content stored on the IT Facilities - The school reserves the right to remove non business-related data from shared areas without notice.

- All access & usage of the system is logged. Although it is not policy to routinely review the usage of the ICT Facilities. The School reserves the right to monitor usage, at any time, for specific instances in which there is good cause for such monitoring or legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee/student wrongdoing, protect the rights or property of the School, to protect the school ICT Facility security, to obtain essential business information after reasonable efforts have been made to contact the user or to comply with legal process.

- The password associated with a particular personal username must not be divulged to another person. Attempts to access, or use, any username which is not authorised to the user are prohibited. Access may be revoked if another user is found in possession of your password.

- Passwords have to be complex and must be at least six characters in length & contain a number. This is enforced by the school's IT system.

- IT Services have the ability to reset lost or forgotten passwords. This will only be done upon verification of ID via the Photo on the schools MIS system.

- IT Services does not allow the connection of non-school owned computer equipment to the network without prior written request & technical approval. This excludes connecting devices via the Schools BYOD (Bring your own device) network, which is covered under the Schools BYOD Policy

- It is School policy to store data on a network drive where it is regularly backed up under the Schools' backup policy

- The School maintains a notification with the Information Commissioner's Office in compliance with the Data Protection Act. It is the responsibility of all School staff to ensure that personal data held and processed is within the terms of the School's data protection policy

- Under no circumstances should you disclose personal or confidential information held on a computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is criminal offence under the Computers' Misuse Act 1990.

- Old Student Accounts will be disabled either on their formal leaving date if midyear or at the start of the next academic year if normal completion. Data files are kept for a period of time under the Schools Backup policy.

- Old Staff Accounts will be disabled on the last day of service. It is the responsibility of the staff member to gather any relevant data, files and e-mails they require during their notice period. This data can be copied by IT services upon request, providing it meets all Data protection obligations. The files relating to this account are kept for a period of time under the School Backup policy.

- Access will not be granted after leaving date. If data is required, the request must be approved by SMT & carried out by IT services

- Access may be revoked at any time if this policy or other school policies are in danger of being or have been breached. This may result in suspension or disciplinary action.

2.8. Wireless Access

- The School supplies two different levels of wireless access; Private WiFi for School devices & WiFi for BYOD

- Private WiFi is configured on school owned devices by IT services. Devices connected to this are treated exactly the same as a wired desktop PC and need to be protected in the same way. Under no circumstances can non-school managed devices connect to this network.

- BYOD access is open to any user with a user account for the IT facilities.

- By connecting to BYOD, users agree to the terms of this document & the BYOD/personal device Policy. It is the responsibility of the individual to ensure their device is free from Viruses and any

other malicious software. IT Services reserve the right to remove this access should it be deemed necessary.

- BYOD has been limited to only allow access to the Internet and other web-based technologies (Such as e-mail) Direct access to file shares (such as network drives) are not permitted and controls are in place to prevent it. Devices cannot access other devices on the BYOD network.

- Users may access files and applications via the Schools remote access facility.

3. Data Security

- You must only access Information held on the School's Computer systems if you have been properly authorised to do so and you need the information to carry out your work

- It is School policy to store data on the school's central servers where it is regularly backed up and secured – Valued Documents should not be stored locally on Desktop PC's, Laptops or Tablets & restrictions are in place to prevent this. Files stored on either are at risk of loss through hardware/software failure or automated administrative activity

- Data may not be stored on non-approved or unmanaged cloud services, such as Dropbox.

- When away from your computer, you must lock your computer (Via the Windows Key + L or Ctrl-Alt-Delete > Lock computer) to prevent unauthorised access to data.

- You must not access personal data whist a device is connected to a projector, as this may result a Data Breach.

3.1 Personal Data and the Data Protection Act

- The school maintains a notification with the Information Commissioner's Office in compliance with the Data Protection Act. It is the responsibility of all School staff to ensure that personal data held and processed is within the terms of the School's data protection policy

- Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access and/or unauthorised modification of data is a criminal offence under the Computer's Misuse Act 1990.

- Under no circumstances should personal or confidential data be stored on or taken offsite via removable media, such as USB sticks or emailed externally. Remote Access provides a secure RDS (Remote Desktop Services) system which should be used if access is required. If there is a

requirement to take any confidential data offsite then please discuss with the Technical Services Manager, to ensure the schools Data Protection Obligations are met.

- Additional Data protection policy & guidance is covered under the school's data protection policy

3.2 Freedom of Information Act

- The school is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities

- Employees should be aware that the act effectivity extends rights available under the Data Protection Act to include all types of information held, whether personal or non-personal. Requests will be dealt with according to the School Freedom of Information Policy

- Staff should note that all data and correspondence, including e-mail messages, held by the School may be provided to a data subject, Internal or external, in the event of a subject access request.

3.3 Anti-Virus Protection, Network Security & Software Updating

- Anti-Virus Software is loaded on all computers as standard and is updated regularly via the Network. There are security protocols in place to prevent users from attempting to remove or disable the Anti-Virus software.

- Non-School Software or data files intended to be run on School equipment by external people such as engineers or trainers must be approved by IT Services & checked for viruses before use. If you suspect that a virus has infected a computer, stop using the computer and contact IT Services immediately. As soon as a Virus is detected, IT services are immediately emailed & an automatic clean-up is attempted.

- Files received by or sent by e-mail are checked for viruses automatically.

- Remote users are responsible for maintaining up to date virus definitions on their own personal devices & can contact IT Services for help as required.

- Vendor provided security updates are installed promptly where necessary.

- The school operates other various security systems, such as firewalls & ACLs designed to ensure the security & safety of the network. Attempting to bypass these will result your access rights being revoked.

3.4 Backup

- All data stored on the School ICT Faculties is backed up under the School's Backup policy. All backup data is stored security & any removable media is encrypted.

4. Email

4.1 Use and Responsibility

- Staff - The School's email system is provided for the School's business purposes and academic support. Limited personal use of the email system is permitted, but not to a level that would influence the primary business purpose. The School will be held liable for any contractual arrangements entered into by email by members of staff if it is reasonable for the recipient to assume that such people are acting with authority (employer's vicarious liability). Such commitments must be avoided at all costs unless specifically authorised.

- Students – The School's email system is provided to aid users with their studies. Personal use of the email is permitted, but the account is only valid whist you are a student at the School.

- You should not use your school email if purchasing personal goods.

- You should not attempt to download email attachments from unverified sources, nor attempt to bypass any restrictions in place to prevent this as this opens the school up to Virus/Ransomware risks. If you are unsure in any way of the validity of an attachment, do not open or download & contact IT Services as soon as possible.

- The email system costs the School time and money, therefor it must be used judiciously in the same manner as other school resources such as telephones and photocopying.

- Email accounts are the property of the School and are designed to assist in the performance of your work. You should, therefore, have no expectation of privacy in any email sent or received, whether it is of a business of personal nature.

- School wide email messages must be business related and of significant importance to all employees.

- Non-School managed email accounts (i.e Personal home email) must not be used for school business or storing school files, as this violates the school's obligation under the Data Protection Act & Freedom of Information Act 2000

- As the school uses "Microsoft Office 365" services for its email, all relevant AUP's and policies set by Microsoft also apply to this document.

4.2 Content

- Email messages must be treated like any other formal written communication. Improper statements in email can give rise to personal liability and liability for the School and can constitute a serious disciplinary matter.

- Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

- Consider carefully before sending confidential or sensitive information via email. Email messages, however confidential or damaging, may have to be disclosed in court proceedings. Please consult IT Services for advice.

- Emails are routinely scanned for the use of offensive language.

- Do not create or send email messages that may be intimidating, hostile or offensive on the basis of sex, race, color, religion, national origin, sexual orientation or disability. It is never permissible to subject another person to public humiliation or ridicule; this is equally true via email.

- Copyright law applies to email. Do not use e-mail to transmit or circulate copyrighted materials.

4.3 Privacy

- Email messages to or from you cannot be considered to be private or confidential

- Although it is not policy to routinely examine the content of individual emails. The School reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee/student wrongdoing, protect the rights or property of the school, to protect the school ICT system security, to obtain essential business information after reasonable efforts have been made to contact the mailbox user or to comply with legal process.

- Messages sent or received may be copied and disclosed by the School for lawful purposes without prior notice. Requests for access/monitoring unless required by law will only be authorized by a member of SMT.

- It is not permissible to access email from another users account either directly or indirectly, unless you obtain that person's prior written approval and a note is made with IT Services.

5. Internet

5.1 Internet & social media

- All Internet usage from the School's network is monitored and logged. Reporting on aggregate usage is performed on a regular basis. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an investigation may result in action via the School's Disciplinary Procedure and possibly criminal investigation.

- Copyright and licensing conditions must be observed when downloading from the internet.

- Once information is published on the worldwide web anyone from anywhere in the world can access it & republish it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites, as this may result in a data protection breach.

- The School operates an open Internet policy & does not actively block access to non-business resources, barring certain categories of content. However, the School reserves the right to remove access to any site(s) which it feels may inhibit the primary business purpose of School.

- All social media accounts used for school business must be registered with the Technical Services Manager. Users must not create accounts using the school's branding without consent.

- Additional Social media access & acceptable use is covered under the School's e-safety policy.

6. Use of personal devices

6.1 Personal Devices/BYOD

- Use of personal devices, such as Laptops, Tablets & Mobile phones are covered under the School's Personal Device/BYOD policy

7. Private use & legislation

7.1 Private Use

- ICT facilities are provided for the School's business and educational purposes and responsible personal use is therefore allowed provided there is no conflict with the interest or requirements of the School.

- The School does not accept liability for any personal loss or damage incurred through using the ICT facilities for private use.

7.2 Other policies & Legislation

- The following are a list of school policies that also apply to the use of the School's ICT Facilities
    - Data Protection Policy
    - E-safety Policy
    - Staff code of conduct
    - Communications Policy

- The following are a list of Acts that apply to the use of the School's ICT facilities:

    - Regulation of Investigatory Powers Act 2000
    - Computers' Misuse Act 1990
    - Protection from Harassment Act 1997
    - Sex Discrimination Act 1975
    - Race Relations Act 1976
    - Disability Discrimination Act 1995
    - Obscene Publications Act 1959
    - Telecommunications Act 1984
    - Protection of Children Act 1978
    - Criminal Justice Act 1988
    - Data Protection Act 1998
    - The Patents Act 1977
    - Copyright, Designs and Patents Act 1988
    - Defamation Act 1996
    - Freedom of Information Act 2000
    - Human Rights Act 1998

8. Conclusion

Compliance with this policy is the responsibility of all users of the school's IT facilities. Any breach of this policy may lead to disciplinary action being taken, access to the School's IT Facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy would be taken up with the Governing Body.

9. Complaints

Complaints will be dealt with in accordance with the school's complaints policy.

10. Review & Updates to this policy

This policy will be reviewed as it is deemed appropriate or changes in the law require it. The policy review will be undertaken by the Technical Services Manager or nominated representative.

11. Contacts

If you have any enquires in relation to this policy, please contact the Technical Services Manager.