POLICY DOCUMENT

Stratford-upon-Avon School is a company limited by guarantee, registered in England and Wales under number 7690776, whose registered office is Stratford-upon-Avon School, Alcester Road, Stratford-upon-Avon, Warwickshire CV37 9DH

Policy Title	ICT NETWORK ACCEPTABLE USE POLICY (AUP)
Policy Reference	**SUAS.SCHOOL.1210.ICT(AUP)01**

DISCLOSABLE UNDER FREEDOM OF INFORMATION ACT 2000	Yes / No	Yes
TO BE PUBLISHED ON WEBSITE	Yes / No	Yes

POLICY OWNERSHIP	
Governor Committee:	School Policy
Department responsible:	Core Leadership Approval
Post-holder: *(Title and Name)*	Mark Grundy (ICT Network Manager)
LINKED PROCEDURES REF:	
Responsible Person - Procedures	N/A

POLICY IMPLEMENTATION DATE:	27/07/2020
PLANNED REVIEW INTERVAL:	Annually
PLANNED NEXT REVIEW DATE:	27/07/2021

Stratford-upon-Avon School welcomes comments and suggestions from the public and staff about the contents and implementation of this policy. Please write to the Compliance Manager at the school address or email your comment to policy@stratfordschool.co.uk.

i. *POLICY OUTLINE*

Applies to: All students both onsite and via external access to the ICT Network services

The School strongly believe in the educational value of electronic services and recognise their potential to support the curriculum. The school provides ICT Network services and equipment that promote the teaching and learning of all learners. Before using any of the provided ICT resources and equipment you must sign and return this form, students will also require the signature and approval of a responsible parent or guardian for their access. This policy covers both internal and remote access to the schools ICT resources.

ii. *PURPOSE*

The policy describes the rules of conduct and expectations on the authorised users of the service and the responsibilities that it places on the user and the sanctions due to a breach of policy or associated policies.

Policies are reviewed on a frequent basis. Relevant documentation is published via the school Website accessed via http://www.stratforduponavonschool.com/School-Policies

RELEVANT LEGISLATIVE ACTS AND REGULATIONS

The relevant acts including *but not limited to*, the

Misuse: The Computer Misuse Act (1990);
Copyright: The Copyright, Designs and Patents Act (1998);
Data Protection: The Data Protection Act (2018);
Defamation: The Defamation Act (1996);
Obscenity: The Obscene Publications Act (1959, 1964); The Protection of Children Act (1978); The Criminal Justice Act (1988);
Discrimination: The Sex Discrimination Act 1975; The Race Relations Act (1976); The Disability Discrimination Act (1995);
Communications: The Telecommunications Regulations (2003).

Criminal Law: Please note that the incitement to commit a crime is within itself a criminal offence The provision of information via a computerised service does fall within this of which such examples would be to place links to illegal or improper sites or links to sites with discriminatory or obscene material.

iii. *IMPLICATIONS OF POLICY*

1. The user is expected to follow all the conditions of the AUP and take a responsible approach to any resources that he/she may have access to.
2. The user is expected to use the ICT Network service for the express purpose of extending their learning or for their professional activities.
3. The user should use their common sense if unsure, if in doubt don't do it and ask a member of staff.
4. ICT Network resources are expensive items in high demand – users are to take care in the use of the equipment and report problems to a member of staff
5. Users are responsible for behaviour and communications over the network. It is assumed that all users will comply with established school standards.

iv. *EQUALITY ANALYSIS*

Stratford upon Avon School believes in equality of access to all students, school staff, visitors and community learners within the school. As such, all staff members have access via the various computing resources within the school and online. All students have access to the ICT suites, the Learning Resource Centre (LRC), various mini ICT Suites located throughout the school and remote services made available from the school. The Learning Support department has its own dedicated computer suite.

v. *CONSULTATION*

Consultation will be with all staff and stakeholders prior to ratification by the Senior Leadership Team.

vi. *PROCEDURE*

Procedure is the method by which the strategic intent of the policy is realised, and is thus an 'instruction manual' on how the policy outcome is to be achieved.

The procedure which supports this policy is within this policy document.

vii. RELATED POLICIES AND PROCEDURES

viii. DOCUMENT HISTORY

The policy will be subject to regular review once ratified by the Senior Leadership Team.
The history of the policy will be recorded using the chart following:

Date	***Author /Reviewer***	***Amendment(s)***	***Approval/ adoption date***
25/02/2019	MGR	• Data Protection Act 2018 • General Data Protection Regulation • Internet and email policy incorporation	
29/06/2020	MGR	• User Accounts • Data Storage • Applications	

RULES FOR GENERAL NETWORK USE

Listed below are a number of general rules but is not an exhaustive list. As appropriate users will be notified regarding suitability or appropriateness when necessary or have individual or group guidance provided.

User Accounts

The issuing of a user account infers compliance with the rules and regulations and as such use is conditional and should not be regarded as a right without responsibilities.

Passwords

- Passwords must be kept secret at all times. If you share your password you are breaching the terms and conditions. Please note that the technical staff members do not need and will not ask for your password as the technical team can reset these if necessary.
- Passwords should be changed frequently, not repeated with minor alterations and contain a number of UPPER CASE and lowercase letters such as numbers and symbols such as !"$%^&*.
- Exceptions to this may be made via requests by ICT Support staff in remote learning situations where access to the school is not possible in order to help troubleshoot a problem. ICT Support staff will make a note of this and ensure any reset passwords are secure and not disclosed to anyone else.

Reset policy

Where it is deemed necessary to reset a users password e.g. a user has forgotten their password – you must notify a member of the ICT Support staff who will reset the password if satisfied with the request and set a prompt for the user to change their password on the next login providing access to site is possible.

Individual use – account sharing

- You DO NOT under any circumstances other people to use your account – this is individual to you and is restricted to you. All monitoring and logging is performed on a user account – if someone else uses your account with your knowledge and does something inappropriate it is still YOUR responsibility.
- If you suspect someone else may have access to your account – please change your password and notify the ICT Support staff IMMEDIATELY so this can be recorded.

Attempting to find another's password

Password cracking or trying to observe/gain another users password is a breach of the Policy.

Temporary accounts

It is necessary at times to create temporary accounts for administrative or demonstration purposes. Access to these accounts is limited and only in consultation with the ICT Support staff.

School Leavers

- Student leavers are to be notified to the ICT Support staff ready for account disabling. It is NOT appropriate to SHARE or PASS ON user account details in the event of a student leaving the school.

Data storage

Once logged onto a PC the following rules apply to data storage and access mechanisms.

Where to store data

- You should store data within your home drive (N:\) or your OneDrive which is a dedicated user storage area for you on a server. Access to student home drives is limited to the student and authorised teaching staff.
- Data stored on your network home drive is backed up both on site and off site for data recovery purposes.
- DO NOT store data ONLY on a Pen drive / flash media / media stick as these should be regarded as TEMPORARY STORAGE media only. We have numerous cases each year of corruption or failures of these devices. We would strongly encourage the use of your OneDrive (available in Office 365) as an alternative.

Anti-Virus

The school provides an Anti-Virus solution to cover the computers (except BYOD client machines). If you are using removable media on your own equipment you should scan the device first. Stratford upon Avon School can NOT give any guarantee that these devices will be 100% virus free so you use these at your OWN RISK.

Authorised file shares

To facilitate the exchange of information shared areas are made available to network users. Folder permissions are set for access to these and various sub-folders/sub-directories within these areas for your use. Please respect this privilege and be aware abuse of this privilege will result in sanctions

Data you are not allowed

Any copyrighted material **IS NOT TO BE STORED** on the ICT Network devices or be accessible via our Services without permission from the ICT Support staff.

Reference should be made under the title 'legal' for further instances of denied materials.

Note. *Downloads of copyright video or music files from Pen Drives or other media devices onto ICT Network storage areas are prohibited.*

Attempts to copy work

Any attempted access to another user's data is prohibited without specific permission from the other user and following approval by the ICT Support staff as regards confidentiality and legality of such.

Applications

Use of / interaction with

Applications on the ICT Network are provided for the educational needs of the users and as such the use of these applications is purely for this purpose. Any attempt to delete or interfere in any way with the installation or operation of these applications. *E.g. deleting shortcuts to commonly used programs is considered a breach of this policy*

Attempted Install of

Applications are only to be installed by the ICT Support staff.
Attempts to install software on ICT Network equipment without prior authorisation (per installable item) is a breach of the Policy.

Games

General

GAMES are **NOT** to be run, downloaded or exchanged on ICT Network resources without specific permission being obtained from the ICT Support staff. Use of games within school is limited to specific departmental educational games and extra-curricular groups/clubs only after the suitability of such has been assessed and formerly approved.

Internet Games

Web based games are prevalent on the Internet – these are banned in the same respect as games above. Use of these web applications are both a breach of this policy and also of the Internet Acceptable Use Policy (Web-AUP) and will result in an immediate Internet ban.

Use of other applications not relevant to the lesson

Use of an existing legitimate application can also be regarded as a sanction event if this is not relevant to the lesson being undertaken or if the responsible adult has directed the user away from the application. *An example would be the use of an Instant Message (IM) client that a user could use during a lesson, or the playing of a music file at an inappropriate time and so the student is 'off task' or causes disruption to a class.*

Malicious

Malicious events are predominately the most serious events within the sanctions given and often require referral to other professional or outside persons.

Hacking attempts

Deliberate attempts to bypass security, unnecessary creation of network traffic by any means (such as DDOS) internally or externally, create user accounts, break passwords, interference with a computers OS, access information from other users or clients are such examples of hacking.

Interference with network infrastructure – cabling

Interference with the infrastructure of the building can be both dangerous to the user and can cause widespread disruption or permanent loss of data for a number of users. As such the user will have serious sanctions imposed in such events.

Disconnection of equipment

As with the above interference category, this puts the user at risk, both in terms of Health and Safety and can cause widespread problems, sanctions are severe.

Theft

As specified under UK law, this is an offence and is reportable to the Police and other associated persons for prosecution or appropriate action after investigation.

Damage

Physical damage (above fair wear and tear) is a reportable event – notifications of damage caused by others must be made as soon as possible so a risk assessment can be made aside from repair. Reports can be made in confidence to a senior member of the ICT Support staff.

Logging on as someone else

Attempted access as another user is a breach of policy for both users, the malicious attempt is often the more serious but the user who allowed their password to become public will face sanctions – Keep your passwords SECRET – the ICT Support staff do not need to know your passwords.

Electronic mail, communication & internet access

Stratford upon-Avon School provides email to assist employees in the performance of their jobs, and students with their learning objectives. Whilst its use should be primarily for Stratford upon-Avon School business, incidental and occasional personal use of email shall be permitted. Stratford upon-Avon School reserves the right to revoke access & monitor content.

- No employee or student shall send, forward or receive emails that in any way may be interpreted as insulting, disruptive or offensive by any other person, or company. Examples of prohibited material include but are not limited to: Sexually explicit messages, images, cartoons, jokes or movie files. Chain Emails. Unwelcome propositions, Profanity, obscenity, slander or libel. Ethnic, religious or racial slurs. Political beliefs or commentary. Any message which could be viewed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.
- Staff should always communicate with students via a shared or departmental mailbox, mail rules are in effect to enforce this within the StratfordSchool.co.uk domain.
- All staff and students shall ensure compliance with relevant legislation
- Internal email and other internal information shall not be forwarded to destinations outside of the Stratford upon-Avon School domain without the authority of the appropriate individual
- Email addresses should not be disclosed unnecessarily. Information provided in surveys or other questionnaires may lead to risks such as receiving unwanted junk messages
- Sensitive information should be communicated as per the GDPR regulations

Internet use

All internet traffic is subject to filtering and SSL interception. Internet is a privilege and NOT a right and so may be withdrawn at any time. Staff and students are expected to use internet access responsibly upholding school values and shall ensure compliance with any relevant legislation. Access to blocked content will be reviewed by the ICT team with input from the safeguarding team.

Legal

Copyright

Copyright material must NOT be used without the author or distributer's permission, to do so is a breach of UK law and school policy.

Music

Music files are also subject to copyright rules as well as other UK legislation and as such MUSIC files THAT ARE NOT CREATED within school are NOT to be stored on the ICT Network without SPECIFIC permission to do so.

Permission will only be granted subject to confirmation that we are authorised and licensed to do so e.g. some software titles include licensed use of music in an education environment subject to specific terms and conditions.

Applications

Applications are subject to numerous copyright and usage laws, terms and conditions and so to attempt to decompile, edit, extract, unauthorised copies or installation of the software is prohibited by law.

Applications on the ICT Network are to be installed only by ICT Network staff or an authorised person NOT a regular user.

Data / Information

Intellectual copyright and proprietary issues are present when any data is transformed into useful information for use within school. Guidance can be sought from the Data protection officer as regards the legal situation.

Commercial

Commercially available material is subject to a number of terms and conditions and guidance must be sought from the ICT Support staff and / or the Data Protection officer about the use, storage or appropriate access to commercial material.

Offensive Material

Offensive material is covered by a number of UK legislative acts and school policies. Please note that remote screen capture technology is present within the school and is monitored on a regular basis. Further guidance is available within the ICT Network Monitoring policy or from the ICT Support staff.

ICT NETWORK ACCEPTABLE USE POLICY (AUP)

Applies to: All STUDENTS both onsite and via external access to the ICT Network services

Rationale

The Network facilities allow students to gain access to their files and shared resources from workstations within the school and from outside across the Internet. Use of the Internet enables students to conduct research, communicate with others and avail of e-Learning opportunities. While there is tremendous potential for good in these facilities, they may be used inappropriately. This policy aims to ensure that the potential for good is realised.

Principles

1. **Access is a privilege and students are responsible for good behaviour in the Network rooms and on the Internet.**
2. **Students are not allowed to have unsupervised access to the Network or the Internet (student activities may be monitored).**
3. **The school can and does track and record information on work carried out on the Network (including sites visited on the Internet) and will delete any files considered to be inappropriate.**
4. **Parental support is sought for upholding high standards.**
5. **Students are required to sign an agreement, which they must honour.**

Rules

Network and Internet users must:

1. **Use only their own name/password and do not share this information with others.**
2. **Never eat or drink in ICT areas.**
3. **Respect ICT equipment and ensure workstations and ICT suites are left in good order.**
4. **Respect copyright laws.**

5. **Access to the ICT Network services is a privilege and NOT a right and so may be withdrawn at any time and without notice.**
6. **Access only their own folders and files and respect the work of others.**
7. **Never send or receive, copy or display offensive messages or pictures.**
8. **Never use ICT systems to harass, insult or attack others.**
9. **Report to their classroom teacher any material which they find upsetting.**
10. **Use the ICT Network services sensibly and take a responsible approach to any resources that you may have access to, including all communications. Expectation of your conduct online are the same as in school.**
11. **Never give out personal details (addresses, telephone numbers etc) of any person in the school.**
12. **Only use e-mail addresses supplied by the school for the purposes intended.**
13. **Use the school network only for work/activities which relate directly to school work or approved activities.**
14. **Consider the environment and do not waste resources (paper, ink, on line time etc.)**
15. **Inform a member of the ICT staff or a teacher if you notice or suspect the following: Damage to ICT equipment, unauthorised access to your account, concerns about any digital content.**

Sanctions

Breaking the rules of any of the ICT Network service policies will involve a punishment of some form depending on how serious this is but includes: -

- **Form Tutor / Learning Mentors for the college informed**
- **Detention**
- **Letters home or a meeting with you, your Parent/Guardian(s) and a senior member of staff with a copy of any digital evidence**
- **Exclusion from school**
- **Notification to others e.g. Police, Social Services**
- **Temporary or permanent ban from internal and/or external ICT Network access**
- **Additional disciplinary action in line with school disciplinary policies**
- **Other external agencies may be contacted**
- **Criminal proceedings instigated**
- **Contributory financial payment(s) to the school**

Acceptance of the terms and conditions below includes adherence to the responsibilities on you/your child as a user of the school ICT Network services.

ICT Network Services TICK □

I wish me/my child to access the school ICT Network services

In ticking the above I hereby agree to the terms, conditions and responsibilities as set out within the school policy, ICT NETWORK Acceptable Use Policy (AUP).

Failure to return a signed form with an appropriate tick will result in the inability to log on to the ICT Network and associated services.

Name of student:

Name of Parent / Guardian:

Signature of Student:

Signature of Parent / Guardian:

DATE:

Please return this page only, duly completed to Student Services.

Failure to return the completed and signed form will deny the user any access of the ICT Network Services.