

Sibford School Student Computer Acceptable Use Policy

Introduction

The use of the latest technology is actively encouraged at Sibford School but with this comes a responsibility to protect both students and the school from abuse of the system.

All students, therefore, must adhere to the policy set out below. This policy covers all computers, laptops and electronic devices within the school, irrespective of who owns the device.

All students are expected to behave responsibly on the school computer network, as they would in classrooms and in other areas of the school.

The Policy:

1. Personal Safety

- 1) Always be extremely cautious about revealing personal details and never reveal a home address, phone number or email address to strangers.
- 2) Do not send anyone your credit card or bank details without checking with a teacher.
- 3) Always inform your teacher or another member of staff if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.
- 4) Always be yourself and do not pretend to be anyone or anything that you are not on the Internet.
- 5) Do not arrange to meet with anyone you have 'met' on the Internet – people are not always who they say they are.
- 6) If someone makes you an offer via email or the Internet that seems too good to be true, it probably is.
- 7) If in doubt ask a teacher or another member of staff.

2. System Security

- 1) Do not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person, or accessing another person's files. Attempting to log on as staff or an ICT administrator will be dealt with severely. You are only permitted to log on as yourself.
- 2) Do not give your password to any other pupil – if you do and they do something wrong while logged on as you, you will be held responsible. If you suspect someone else knows your password it will need to be changed by an ICT administrator.
- 3) Do not make deliberate attempts to disrupt the computer system or destroy data e.g. by knowingly distributing a virus.
- 4) Do not alter school hardware in any way.
- 5) Do not tamper with or remove any cables etc that are attached to school equipment.
- 6) Do not misuse hardware; treat equipment with care and respect.
- 7) Do not attempt to connect to another student's laptop or device while at school. You are not permitted to establish your own computer network.

- 8) Do not eat or drink whilst using computer equipment.
- 9) Do not use email or Internet during lessons unless a member of staff has given permission.

3. Inappropriate Behaviour

(All inappropriate behaviour is against school rules and will result in serious sanctions. Here, inappropriate behaviour relates to any electronic communication device.)

- 1) Do not use indecent, obscene, offensive or threatening language.
- 2) Do not post or send information that could cause damage or disruption.
- 3) Do not engage in personal, prejudicial or discriminatory attacks.
- 4) Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
- 5) Do not knowingly or recklessly send or post false, defamatory or malicious information about a person or about school.
- 6) Do not post or send private information about another person without their agreeing first.
- 7) Do not use the Internet for gambling.
- 8) Bullying of another person either by email, online or via texts will be treated with the highest severity AND is against the law. The Police will follow up any infringements or harassment.
- 9) Do not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people.
- 10) If you mistakenly access such material please inform your teacher or another member of staff immediately, or you will be held responsible.
- 11) If you are planning any activity which might risk breaking the Acceptable Use Policy (e.g. research into terrorism for a legitimate project), a member of staff must be informed beforehand and give permission.
- 12) Do not attempt to use proxy sites on the Internet.
- 13) Do not take a photo of another student or member of staff without their permission. NO PHOTOGRAPHS or VIDEOS to be taken of other pupils without the permission of staff and the pupil concerned.
- 14) Do not load photos of other people to web sites or social networking sites

4. Email

- 1) Do not reply to spam mails as this will result in more spam. Delete all spam mails.
- 2) Do not open an attachment from an unknown source as it may contain a virus.
- 3) Do not send, by email, any files greater than 5mb.
- 4) Do not send or forward annoying or unnecessary messages to a large number of people e.g. chain mail.
- 5) Observe good housekeeping practice with emails; delete old mail.

5. Plagiarism and Copyright:

- 1) Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the Internet or anywhere else. This could result in disqualification from Exams in the case of coursework.
- 2) Respect copyright. Breaking copyright law occurs when you reproduce a piece of work that is protected by copyright. If you are unsure whether or not you can use a piece of work, you should request permission from the copyright owner. This includes music files and the copying of CDs etc.

6. Privacy:

- 1) All files and emails on the system are the property of the school. As such, system administrators and staff have the right to access them if required.
- 2) Do not assume any email sent on the Internet is secure.
- 3) All network access, web browsing and emails on the school system are logged and may be routinely monitored on any computer screen without the student's knowledge.
- 4) If you are suspected of breaking this policy, your own personal laptop/device and mobile phone can be searched by staff and your parents will be informed.
- 5) The school reserves the right to randomly search the Internet for inappropriate material posted by students and to act upon it.

7. Software:

- 1) Do not install any software on the school system.
- 2) Do not attempt to download programs from the Internet onto school computers.
- 3) Do not knowingly install spyware or any sort of hacking software or device.

8. Sanctions:

- 1) Sanctions will vary depending on the severity of the offence, from a warning or withdrawal of Internet use, to suspension or expulsion. Any breach of the law may lead to the involvement of the police.

9. General and Best Practice:

- 1) When printing, only print one copy and ensure your name appears on every printout.
- 2) Always log off your computer when you have finished using it.
- 3) Save work regularly using sensible file names.
- 4) Always back up any work that is not saved onto the school network.
- 5) Avoid saving files larger than 5mb.
- 6) Observe health and safety guidelines when using computer equipment.
- 7) Be considerate and polite to other users.
- 8) Leave your computer and the surrounding area clean and tidy.

- 9) When you leave school for good ensure you save any files you wish to take with you as your account will be deleted.
- 10) Always abide by the ICT Code of Conduct.

10. Other Electronic Devices:

The above ICT Policy also covers other electronic devices such as laptops and mobile phones while used at school. However, none of these devices are covered by the school's insurance and the school accepts no liability for them. All devices should be security marked and kept locked away where possible. This also includes items such as digital cameras and personal DVD players etc.

- 1) If you wish to use your own personal laptop you can only connect via the student network service. You must use wireless connectivity – do not cable your laptop to the network.
- 2) Your laptop must have up to date anti virus software installed.
- 3) Do not attempt to use hacking tools.
- 4) The use of webcams is not permitted.
- 5) You are expected to abide by the Laptop Code of Conduct.
- 6) Do not use a mobile phone during lessons.
- 7) Do not take photos or videos, using a phone, in school unless a member of staff has given permission.
- 8) Do not photograph or video people without their permission.
- 9) The use of music/video players e.g. ipods is banned during lessons unless a teacher has given permission.
- 10) Do not connect music/video players to the school network or school computers.

The use of the latest technology is actively encouraged at Sibford School but with this comes a responsibility to protect both students and the school from abuse of the system.

All students, therefore, must adhere to the policy set out below. This policy covers all computers, laptops and electronic devices within the school, irrespective of who owns the device.

All students are expected to behave responsibly on the school computer network, as they would in classrooms and in other areas of the school.

Student:

I have read and I understand the school's Computer Acceptable Use Policy. I agree that I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed _____

Print Name _____

Date _____

Parent/Guardian

As a parent or Guardian I have read this agreement. I understand that although Sibford School employs the latest filtering and security technology no system can be 100% safe. I give my child permission to use the school computer system.

Signed _____

Print Name _____

Date _____

Please complete this page of the policy and return it to Sibford School if you have not done so earlier. The policy document should be kept by you.