SPALDING GRAMMAR SCHOOL ICT ACCEPTABLE USE POLICY

SUMMARY FOR ALL USERS

Spalding Grammar School provides access to networked computers to support students' academic work. ICT is an enormously useful tool for learning and most users derive huge benefits. There are nonetheless significant risks of unacceptable and potentially dangerous misuse which require safeguards and guidance to help avoid the dangers. Our Acceptable Use Policy is an extension to the School Code of Conduct, includes guidelines for the safe and responsible use of the network and the Internet and identifies those activities which constitute an abuse of ICT facilities. We ask you to read it carefully and sign and return the last page. Copies of the policy can be found on the school website in the 'INFO FOR PARENTS' section.
In summary, users of the school network are prohibited from:
• logging on to the network with another user's account
• creating or sending offensive or harassing materials to others
• altering the settings of school computers or making other changes which render them unusable by others
• tampering physically with the equipment
• installing software without authorisation (including games on memory sticks)
• hacking into unauthorised areas of the network
• accessing inappropriate websites or trying to circumvent the school filtering system
• attempting to spread viruses via the network
• any form of illegal activity, including software and media piracy

Disciplinary action will be taken against those found to be in breach of the Acceptable Use Policy.

FULL POLICY: STUDENTS

This policy is an extension of the School Code of Conduct, covering specifically the use of the Spalding Grammar School network and any computer equipment connected to it. For the purpose of this document, the term *mobile device* will include laptops, netbooks and electronic notebooks, PC tablets, mobile phones, games consoles or any other portable web-enabled computing device.

Section A - Computer Facilities

1. Overview

Every pupil is issued with a username, password and an email address at the start of his school career. This provides access to the computer network and a range of standard applications (word processing, spreadsheet, database etc.) as well as online facilities such as the intranet, Internet and electronic mail. A public wireless network enables users to connect with their own mobile devices. School ICT facilities are provided to support pupils' study in all subjects, and priority will always be given to those using computers for academic and other school-related work. Recreational use of the network is permitted within clearly stated limits and may vary from one area of the school to another. Access to the computer network is a privilege and it is the responsibility of pupils to restrict themselves to usage which is ethical and appropriate. **Failure to comply with this policy will result in disciplinary action.** Those administering the school network are responsible for ensuring the security of user data, and pupils can assume that their files and information are protected from viruses and from interference by others. They should not, however, assume that their activities are completely private. Staff are authorised to monitor all user accounts to ensure the security of the network; records of usage, stored files and email messages that have been sent or received may be scrutinised at any time (a) during routine system maintenance or (b) if there is reason to suspect misuse of the network. All pupil machines are monitored by software and inappropriate activity is reported to the Head of ICT.

2. Rules

a. General Conduct and Use

i. Pupils should conduct themselves in an orderly and quiet fashion, and must always show consideration for other users.
ii. No food or drink may be consumed.
iii. Any damage to computers, furniture or fitments should be reported to a member of the ICT team or other member of staff without delay. The same applies to any apparent malfunction of equipment.
iv. Pupils using computers before school and during morning break, lunch break and private study periods should leave the computer rooms in time to arrive punctually for their next timetabled commitment.
v. Only one pupil should be seated and working at a computer at any one time.
vi. Chairs should be placed tidily in computer rooms before leaving.
vii. Pupils are responsible for backing up important files and documents. The school is not liable for lost, damaged or unavailable information for whatever reason.

b. Use of the Network

i. When logging on to the network (including logging on from home), a pupil must always use his own user identification and password. Any attempt to impersonate another user will be treated as a serious offence, as will any attempt to interfere with data stored on the network by another user. These activities are in fact illegal under UK law.
ii. Never, under any circumstances, use another person's account or attempt to log on as a system administrator.
iii. Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user. The network or other networks connected to the Internet must not be vandalised. This includes the uploading or creating of computer viruses.
iv. Harassment is defined as the annoyance of another user, or interference with another
user's work. Harassment must never occur; this includes, but is not limited to, the sending of unwanted email (see below).
v. If a pupil identifies a security problem on the system he must notify staff immediately. He/she must not demonstrate the problem to other users.
vi. Students must never divulge their passwords to other users or to users of computers outside the school. Any pupil who suspects that this has happened accidentally should change his/her password without delay.
vii. Before leaving a computer, pupils must always log off the network and check that the logging out procedure is complete.
viii. Pupils must not attempt to gain access to the local drive of any machine or to create local accounts (administrative or otherwise).
ix. It is strictly forbidden to attempt to share drives, folders or files across the network other than via the network.
x. Only software that has been provided on the network may be run on school computers; this includes programmes run from USB devices, which should only be used for the transfer of data. Pupils are not permitted to import or download applications or games. In many cases it is illegal to do so.
xi. You are reminded that it is a breach of the School Plagiarism Policy (and of the rules of examination boards) to pass off another's work as your own. This includes copying and pasting information accessed online without proper acknowledgement.
xii. Pupils must be aware of, and comply with, the restrictions placed on certain kinds of usage; notably the playing of games and visiting social networking sites on particular machines and at particular times of the day, where priority is given to academic work.

Section B - Internet and Email

1. Overview

The School manages its own Internet access and will block access to web sites known to contain offensive or inappropriate material. The filter is continually updated, though there can be no absolute guarantee that unsuitable material is never available. Pupils are given training in safe and effective use of the Internet at various stages in their school career.

2. Rules

a. General Netiquette
Pupils must not:
i. Send electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable.
ii. Disclose to a third party the personal details of any other pupil.
iii. Access any inappropriate Internet site.
iv. Breach another person's copyright in any material.
v. Upload or download any unauthorised software or attempt to run that software. In particular hacking, encryption and other system tools are expressly forbidden.
vi. Purchase goods or services via the computer network.
vii. Use the computer network to gain unauthorised access to any other computer network.
viii. Attempt to spread computer viruses.
ix. Engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden, as of course is any threatening or obscene matter.

b. Personal Safety
Pupils need to be aware that thoughtless use of email and the Internet may jeopardise their personal safety either at school or outside school. Pupils should therefore:
i. Be aware that any person they "meet" or communicate with online may pretend to be someone else.
ii. Never arrange a meeting in person with anyone they have "met" or only communicated with online without prior parental approval.
iii. Not respond to messages or bulletin board items that are indecent, suggestive, belligerent, discriminatory, threatening, or which make the student feel uncomfortable or unsafe in any way. If such a message is encountered the pupil should report it to his form tutor and parents or via an online reporting service such as ThinkUKnow (http://www.thinkuknow.co.uk).
iv. Remember that anything they read online may not be accurate.
v. Ignore offers that involve either financial transactions or personal meetings.
vi. Not disclose any personal details online, such as their home address or telephone number.

Section C – Mobile devices

1. Overview
Pupils may connect mobile devices to the school's public network. This provides filtered access to the Internet and the school's portal.

2. Rules
These rules apply to all mobile devices:
a. Pupils may only connect their own devices to the school's *public* network.
b. Under no circumstances should computers, printers or other devices be detached from the network to make way for a pupil's own computer or mobile device.
c. No mobile device may be plugged directly into any network switch, hub or router.
d. The sharing of local drives, folders or files across the network is strictly forbidden.
e. No servers of any description should be attached to the network.
f. Pupils should ensure that their own devices are properly protected from viruses before connecting to the school public network.
g. Pupils are responsible for the material that exists on or is accessed via their mobile device. The ICT team is empowered to scrutinise, and if necessary retain for further investigation, any device which is or has been attached to the network.
h. The school cannot accept responsibility for any damage, howsoever caused, to pupils' own mobile devices or their contents (files, folders etc.).
i. All rules of usage for Internet access and computer usage continue to apply.
j. It is the responsibility of the owner to ensure that he has a licence for all software installed on his mobile device.
k No software should be run on a mobile device during lessons which is not appropriate to that lesson.

Spalding Grammar School ICT Acceptable Use Policy supersedes all previous agreements.

E-MAIL
Because of the nature of the organisation, any e-mail or attachments are considered the property of the school and may be monitored, especially as the school acts in loco parentis. Any findings will remain confidential, but disciplinary action may be taken for inappropriate use of the system. This would include any students found to be deliberately sending offensive messages, 'spamming' the system or using other people's e-mail login names. Students must not open any e-mail where the content is suspicious nor open suspect attachments without speaking to the Network management staff.

INTERNET
Students are expected to use the Internet appropriately. They are encouraged and have the right to examine a broad range of information, opinions and ideas for the purpose of educational research. They have a responsibility to ensure their use is educational and ethical. Students should not communicate with strangers unless with the permission of staff and should avoid giving personal or financial details. It is unacceptable to access chat rooms or messaging services unless instructed by a member of staff; personal photos should not be sent without parental agreement; unacceptable websites should not be accessed; games simulations or software must not be downloaded; obscene, vulgar or inappropriate language or material must not be used or transmitted. Users should report misuse of the Internet to staff. Teachers and the school will determine what is appropriate material and use and shall not be held liable for any materials retrieved from the Internet by students.

I have read the Acceptable Use Policy and I undertake to abide by it. I accept that the school is not liable for lost, damaged or unavailable information due to technical or other difficulties and is not responsible for what users do or the information they access. I acknowledge that the majority of such information is generated outside of school control.

I fully understand that if I do not abide by this Acceptable Use Policy, my access privileges may be withdrawn and that disciplinary or legal action may be taken against me. When unsure of any procedure or policy, I accept it is my responsibility to ask a member of staff. I will not use other people's passwords nor communicate my passwords to anyone else.

I understand that all staff have the right to access my work on the school network at any time without prior warning.

Student name: ……..

Student signature: ……. Date : ……

Parent/Guardian:
As parent/guardian of the above student, who is under the age of 18, I understand all of the above and accept full responsibility for my son or daughter's actions.

Signature: ……..…….. Date : ……..