Spalding High School

Acceptable Use Agreement

Introduction

**Please read this "Acceptable Use" document carefully. It is designed
to explain the use of Computer Networks within Spalding High School and the
responsibilities that you as a student are required to observe, in its use. This Acceptable
Use Agreement is underpinned and supported by both the School's Behaviour Policy and
Personal Electronic Devices and Mobile Phone Policy. Students and Parents should read
both policies in full on the school website.**

Scope

The following rules and procedures have been formulated to ensure a clear understanding of the
responsibilities in the use of the school computer system, e-mail and Internet facilities and applies
to all students.

It applies to all computer software and hardware provided by the school including Personal
Computers, Laptops, Wireless & Broadband connections, Servers and any other equipment that
may be provided for use and for Special Educational Needs.

In reference to the School's Personal Electronic Devices (PED), Mobile Phone and Social Media
Policy; No PED is to be charged in school. No PED (including mobile phones) are to be connected to
the school system, wi-fi or Internet. Students should remember that they have all signed an
Acceptable Use Policy which specifies the use of technology and school systems.

Email and Internet

- The email and Internet system is provided for education purposes only and should not be used
  for personal gain or reward.

- Sending messages of an abusive, offensive, harassing, racist, discriminatory or obscene nature is
  not permitted and will result in disciplinary action which may include withdrawal of access
  rights. Should the school receive evidence that any comment, image or recording judged by us
  to be inflammatory, threatening, malicious or offensive about a named pupil, member of staff
  or the school itself be placed in the public domain, then action will be taken. This action may
  include a formal report or complaint to the police.

- Access to the Internet is restricted and filtered on content and is available for suitable
  educational requirements. Accessing or attempting to access, downloading and/or uploading
  abusive, offensive, obscene or illegal material is strictly forbidden and pupils must follow
  guidelines from teachers in lessons where access to online digital resources (e.g. webpages and
  YouTube content) are being used to enhance teaching and learning.

- It is important that care should be taken when downloading material from the Internet that
  copyright notices and license implications are observed.

- Personal use of email and the Internet is permitted, provided it is carried out in the student's
  own time, during non contact periods (Sixth Form), out of normal school hours, or by prior
  arrangement with a member of staff.

Cyberbullying

- Cyberbullying is the sending or posting of harmful or cruel text messages and/or images, using the Internet or other digital communication devices.

- Spalding High School does not tolerate bullying in any form. Any student found to be involved in incidents of cyberbullying will be dealt with firmly.

- The School Behaviour Policy and Personal Electronic Devices, Mobile Phone and Social Media Policy sets out clearly the procedures and sanctions available to staff to deal with incidents of cyberbullying.

Monitoring

- The school maintains security and anti-virus software that monitors and records details of all network activity in which individuals transmit or receive files and data.

- To ensure that the rules and procedures are being followed, both email and Internet use will be monitored on a regular basis. This will include the access of Internet sites and email sent or received though school servers.

Security and Confidentiality

- Every user will be issued with a unique user name and password; this must be **kept confidential**, not written down or given to others. The password should be changed on a regular basis in accordance with the system default password expiry period.

- Each user will have their own area on the network for the storage of data files, coursework and email. The IT Manager and associated staff will at times randomly inspect data stored on the school networks to check appropriate content of such data.

- Screens should never be left unattended and after use, all computers should be logged off from the network.

- For personal safety, any form of electronic communication should have no references to personal information such as student home addresses, telephone numbers etc.

- It is the responsibility of all students to protect the security and confidentiality of the school networks. Students must not try to deliberately access the online files and folders of their peers, teachers or others.

Failure to abide by this policy on acceptable use will result in disciplinary action, which may include withdrawal of access rights. In serious cases it may result in legal action.

You are now requested to sign your acceptance of this policy and agreement document. This has been provided in the form of a separate page accompanying this document, such that the student can **keep the actual policy for reference** and the signed portion can be filed with student records for future use. A summary of this policy can also be found in the school planner.