Rules for ICT Users - Staff

	Notes
1	You must not use, or try to use, Sir Thomas Boughey High School's e-mail and internet facilities to create, distribute or display in any form any material that is or may be considered to be illegal, offensive or unacceptable under our rules and policies. It is impossible to give a complete list of what is considered offensive or unacceptable, but the following are included (and in some cases may also be illegal). Anything that: • is pornographic or obscene, or includes any form of sexually explicit humour; • is intimidating, discriminatory (for example, racist, sexist or homophobic) • is defamatory, encourages violence or strong feelings; • is hateful; • is fraudulent; • shows or encourages violence or criminal acts; • may give Sir Thomas Boughey High School a bad name; or is a deliberate harmful attack on systems Sir Thomas Boughey High School use, own or manage.
2	Attempts to access unacceptable internet content will be treated the same whether the attempt was successful or not. Terms entered into search engines such as "google" can be recorded and they will be considered as seriously as the content that would result from the search even if the content is blocked.
3	You must not use the e-mail or internet facilities for time-wasting activities, such as chain letters, or for sending private e-mails to everyone on the global address list.
4	You must not use or try to use Sir Thomas Boughey High School ICT systems to access, without permission, any e-mail that is intended for another member of staff or an e-mail account of another member of staff.
5	Ensure you know who is in charge of the ICT system you use, i.e. the System Manager.

6	You must be aware that any infringement of the current legislation relating to the use of ICT systems :- Data Protection Acts 1984 & 1998 Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 The Telecommunications Act 1984 Breaches of this legislation may result in disciplinary, civil and/or criminal action.
7	You must follow any local rules determined by the Headteacher in relation to the use of private equipment and software. All software must be used strictly in accordance the terms of its licence and may only be copied if specifically approved by the System Manager.
8	You must ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. This includes if you are accessing systems from outside the school including at home. Do not leave you computer logged on, i.e. where data can be directly accessed without password control, when not in attendance.
9	You must not leave any computer unattended if you are accessing school systems on it unless the screen is locked i.e. it requires a password to gain access. This includes if you are accessing systems from outside the school including at home.
10	You must not exceed any access rights to systems or limitations on the use of data imposed on you by the System Manager. The ability to access information or systems is not the same as having authorisation to do so.
11	The System Manager will advise you on the frequency of your password changes. In some cases these will be enforced by the system in use. You should not re-use the same password and make sure it is a minimum of 6 alpha/numeric characters, ideally a mix of upper and lower case text based on a "made up" word, but not obvious or guessable, e.g. surname; date of birth.
12	You must not share your user name and password with **ANYONE** unless specifically authorised to do so by the System Manager, e.g. in cases of shared access
13	Do not write your password down. You will be directly accountable for any network activity including internet and email use by your account.
14	The System Manager will advise you on what "back ups" you need to make of the data and programs you use and the regularity and security of those backups.

15	You must ensure that newly received USB memory sticks, CD ROMs and emails have been checked for computer viruses. Any suspected or actual computer virus infection must be reported immediately to the System Manager.
16	You must be vigilant for any suspicious ICT activity. You must immediately report any suspected or actual breach of ICT security to the System Manager or, in exceptional cases, the Headteacher.
17	You must be aware that the data you create with Sir Thomas Boughey High School equipment and systems remains the property of Sir Thomas Boughey High School. All data must be handled in accordance with any Protective Marking Scheme that may be in place.
18	You must keep all business-related data on the Sir Thomas Boughey High School network and not on the hard drive of your PC. Data that is stored on the Sir Thomas Boughey High School network will be backed up on a regular basis
19	You must lock sensitive data (hard copy and disks) away when not in use.
20	You must ensure that sensitive data, both paper-based and electronic is disposed of properly – shred hardcopies and destroy disks.
21	You must not store large amounts of personal data (non Sir Thomas Boughey High School work) files including but not limited to personal MP3 files, personal photographs, personal music files and personal documents on the Sir Thomas Boughey High School network. Sir Thomas Boughey High School will not be held responsible for the deletion of any personal data.
22	You must make yourself aware of the contents of all other ICT related policies.
23	You must not copy files that are accessible centrally on the Sir Thomas Boughey High School network onto your personal home drive on the network unless for amendment after which they must be deleted from the home drive. Wherever possible, work must be kept on shared network drives and not on your home drives
24	You must ensure that any data you take off site be it on a laptop, USB storage device or any other media is encrypted.

Staffordshire County Council - ICT Security Policy for Schools

Rules and Agreements for Staff

Staff Declaration

You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in your personal file.

Declaration

I confirm that, as an authorised user of the School's ICT facilities, E-mail and Internet services, I have read, understood and accepted all of the Rules for ICT users – Staff.

Your details

Name:

Job title:

Signature: Date: