



Reason for a Code of conduct

- To ensure that the computing environment is as safe as possible
- Set ground rules to help maintain such a safe environment

Keeping the Code of Conduct current

- This is a constantly evolving document
- The latest version will always be applied, irrespective of which version was signed. Staff will be notified of changes 1 month prior to new version becoming effectively "Live"
- The latest version will always be available on the school's web site (<http://www.chilton-trinity.co.uk>)
- The spirit of the code will be applied to all unforeseen future incidents

What the school does to safeguard the staff

- Staff are given a secret password to access the school network and e-mail
- Subscribes to a filtered e-mail system with staff given a unique @chilton-trinity and County @educ.somerset.gov.uke-mail address
- Subscribes to a nationally recognized Internet filtering service
- Monitors and logs all Internet usage

Ownership of files

- All files on the school network are the property of the school
- All files can be examined at any time
- Files deemed: offensive, inappropriate or irrelevant will be deleted without prior notice

What is expected from the staff

- To follow the code of conduct
- Be responsible for their own actions when using the computer network, E-Mail and Internet
- Inform a member of the Senior Team immediately if an inappropriate website is accidentally accessed
- Keep passwords secret as all computer access using a member of staff's unique identity and secret password is assumed to be carried out by that member of staff.



The spirit of the code of conduct

“The spirit of the code of conduct will be applied to all unforeseen future incidents”

1	Passwords	<ul style="list-style-type: none"> • Never tell anyone your password under any circumstances whatsoever. • Change passwords regularly (or if you think somebody knows it). • Do not access the network using any account other than your own. • Do not attempt to guess another account’s password.
2	Security	<ul style="list-style-type: none"> • Do not try to bypass the school’s network security or Internet filtering. • Do not attempt to infect the school’s network with Malware. (Malicious Software) • DO not try to reconfigure the computer settings. • Always lock (or log-off) your computer when leaving it (even if for a short time)
3	Internet	<ul style="list-style-type: none"> • Do not try to access inappropriate images (and should such images appear by accident report the fact immediately to Ben Parnell). • Do not use personal e-mail accounts (Gmail, Yahoo, Microsoft etc.) to communicate with students. • Do not have students as friends on any social media site (Bebo, Facebook, MySpace etc.).
4	E-mail	<ul style="list-style-type: none"> • Never send abusive E-mails/messages. • Only ever use the filtered E-mail system provided by the school for school business. • Only open E-mail attachments if you know, and trust, the sender of the E-mail.
5	Social Networking	<ul style="list-style-type: none"> • Avoid using Chat rooms, Forums or Blogs unless this has been approved by ICT – we need to ensure accountability and safeguarding.
6	Hardware Software Copyright	<ul style="list-style-type: none"> • Do not: Damage, deface or unplug the computers. • Never try to install software on the school network. (Games, music, Sync’ phone, iPod etc.) • Copyright is very serious. If in doubt do not use the material.

I acknowledge that I will be held responsible for my own actions whilst using the school network and computer access using my unique identity and password.

Staff Name: _____

Staff Signature: _____

Date: _____

