TOR VIEW
A SPECIALIST LEARNING COMMUNITY

ACCEPTABLE INTERNET USE POLICY

The computer system is owned by Tor View School and is made available to staff to enhance their professional activities including teaching, research, administration and management. Tor View School is keen to see staff make full use of the system, in order that they might broaden their skills and enhance their professional development.

Tor View School's Internet Access Policy has been drawn up to protect all parties. With the agreement of the Headteacher, the system and internet access can be made available for occasional personal use, during the employee's own time i.e. after school and during the lunch break. Staff are reminded that inappropriate use of the internet could result in action being taken under the terms of the School's disciplinary procedure. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Therefore, it is important that all staff familiarise themselves with the principles set out below:

- All Internet activity should be appropriate to staff professional activity, including research for professional purposes. Where the system is made available for personal use, the same principles apply.
- Under the terms of the Authority's Trade Union Facilities Agreement, reasonable use of computer facilities for authorised trade union representatives is permitted.
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems and laptops, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mails sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;

- Posting anonymous messages and forwarding chain letters is forbidden;
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Access to You Tube content is restricted to lesson times only to ensure that pupil use can be supervised by staff. By default, access will be unavailable throughout the day unless specifically requested by a member of staff via the IT Helpdesk.

The following guidelines (some of which also apply to other forms of correspondence) tell you what is and what is not good practice when you use internal or Internet E-mail services.

You should:

- check your E-mail inbox for new messages regularly;
- treat E-mail as you would a letter, remember they can be forwarded / copied to others;
- check the message and think how the person may react to it before you send it;
- make sure you use correct and up to date E-mail addresses;
- file mail when you have dealt with it and delete any items that you do not need to keep;

You should not:

- use E-mail to manage staff where face-to-face discussion is more appropriate;
- create wide-distribution E-mails (for example, to addressees throughout the world) unless this form of communication is vital;
- print out messages you receive unless you need a hard copy;
- send large file attachments to E-mails to many addressees;
- send an E-mail that the person who receives it may think is a waste of resources;
- use jargon, abbreviations or symbols if the person who receives the E-mail may not understand them.

Please see ICT Security Framework Policy for paragraph references.

	Notes	Paragraph Reference
1.	Ensure you know who is in charge of the ICT system you use, i.e. the ICT Network Coordinator.	4.5.1
2.	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 Provisions of this legislation may result in disciplinary, civil and/or criminal action.	5.1.2
3.	ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and as such all users have a personal responsibility for ICT security. Consequently, you must ensure that you receive appropriate training and documentation in the use of your ICT system and in the protection and disclosure of data held.	5.2.2, 6.2, 6.3 & 6.4
4.	Follow the local rules determined by the Principal 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.	5.4.4 & 8.2.1
5.	Ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. Ensure that equipment is sited so as to avoid environmental risks, e.g. dust, heat. Do not leave your computer logged on, i.e. where data can be directly accessed without password control, when not in attendance. These same rules apply to official equipment used at home.	7.2.1
6.	You must not exceed any access rights to systems or limitations on the use of data granted to you by the System Manager.	8.4.1

7.	The ICT Network Coordinator 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. Do not divulge your password to any person, or use another person's password, unless specifically authorised to do so by the ICT Network Coordinator, e.g. in cases of shared access. Do not write your password down, unless it is held securely on your person at all times or kept in a locked receptacle/drawer to which only you have access.	8.6.1
8.	The ICT Network Coordinator 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.	8.7.1
9.	Ensure that newly received CD ROMs and emails have been checked for computer viruses. Any suspected or actual computer virus infection must be reported immediately to the ICT Network Coordinator.	8.8.1 & 8.8.2
10.	Due regard must be given to the sensitivity of the respective information in disposing of ICT printouts, CDs, etc.	8.9.1
11.	Users must exercise extreme vigilance towards any suspicious event relating to ICT use and immediately report any suspected or actual breach of ICT security to the ICT Network Coordinator or, in exceptional cases, the Principal, Chair of Governors or Internal Audit.	9.1
12.	Users of these facilities must complete the ‘Staff Declaration Form’.	10.1

Tor View School **Responsible E-mail and Internet Use** Please complete, sign and return to the school office	
Name:	Address:
Agreement I have read and understand the school 'E-mail and Internet Use Good Practice; E-mail and Internet Acceptable Use; and Rules for ICT Users' documents. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
Signed:	Date:

	Name/Initials:	**Date:**
Written By:	Tor View	
Reviewed:	Kelly Morgan	18.04.18