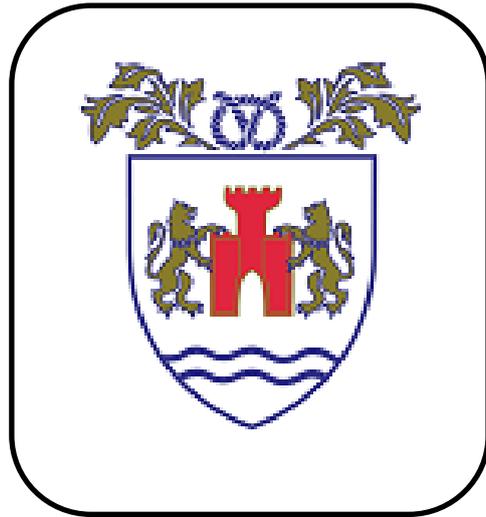


Wolstanton High School



Students

IT Policy

Contents:

1. [Overview](#)
2. [Policy](#)
3. [Procedure](#)
4. [Authorised use of the IT facilities](#)
5. [Authorised use of the communications facilities](#)
6. [Unauthorised use of the IT facilities](#)
7. [Unauthorised use of the communications facilities](#)
8. [Implementation of the policy](#)
9. [Encryption](#)
10. [Backups](#)
11. [Remote Access](#)
12. [General IT information](#)

Statement of intent

Wolstanton High School believes that IT plays an important part in both teaching and learning over a range of subjects.

Wolstanton High School is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

This policy covers the rules and procedures for authorised and unauthorised use of the IT and communication facilities and is implemented in conjunction with Wolstanton High School's E-safety Policy.

Signed by

_____ Headteacher

Date: _____

_____ Chair of Governors

Date: _____

Next review date: _____ Autumn 2018 _____

1. Overview

- 1.1. The IT facilities at Wolstanton High School are defined as:
- Computers and software
 - Monitors
 - Keyboards
 - Mouses
 - Printers
 - Scanners
 - Cameras
 - Camcorders
 - Other devices including furnishings and fittings used with them
- 1.2. The communication facilities at Wolstanton High School are defined as:
- Telephones
 - Fax machines
 - Mobile phones
 - Other devices including fittings used with them
- 1.3. Internet and e-mail can be defined as a communication facility used in conjunction with IT facilities; as such, these will coincide with the IT facilities.
- 1.4. This policy contains:
- Wolstanton High School's view on the use of e-mail and the internet at work.
 - An explanation on what you can or cannot do.
 - The consequences if you fail to follow the rules set out in this policy.
 - General information relating to IT, including the Data Protection Act.
 - How the policy is implemented.

2. Policy

- 2.1. Wolstanton High School will provide a wide variety of computing resources which are under constant review to ensure improvement and development.
- 2.2. Students are offered access to the Schools network, internet and email services.
- 2.3. Abuse of the IT facilities could result in access being removed. Students should always be aware of IT use, and misuse of the facilities, as defined in this policy.
- 2.4. This policy applies to any device connected to Wolstanton High School's network.
- 2.5. Any breach of the rules in this policy will be dealt with by the behaviour policy.
- 2.6. Access to the school network, internet and email services will stop once students have left the school.

3. Equipment

- 3.1. IT Facilities may only be used for school work
- 3.2. All school computer equipment should be treated with care and respect.
- 3.3. Students should not attempt to move or change the setup of the devices in anyway.
- 3.4. Any damage should be reported to your teacher immediately.

4. Security

- 4.1. Students must keep their passwords secret, do not share your password with anyone, students, teachers or IT staff do not need your password.
- 4.2. Students should not log on or attempt to logon as another person.
- 4.3. Passwords are required to be 6 characters minimum and for best practice include a combination of letters and numbers.
- 4.4. Password should be changed regularly.
- 4.5. School network access is restricted; students should not try to bypass any security that is implemented at Wolstanton High School.

5. Unauthorised use of the IT facilities

- 5.1. It is not permitted under any circumstance to:
 - 5.1.1. Damage any computing equipment – ie damage to keyboard, mice, PCs, tablets or any other device.
 - 5.1.2. Attempts to bypass the network security.
 - 5.1.3. Bullying online either via Email or other communications.
 - 5.1.4. Use or attempt to use someone else's user account. All users of the IT facilities will be issued with a unique user account and password. The password must be changed at regular intervals. User account passwords must never be disclosed to or by anyone. This is illegal under the Computer Misuse Act.
 - 5.1.5. Use the IT facilities at any time to access, download, send, receive, view or display any of the following:
 - Any material that is illegal
 - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations

- Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
 - Online gambling
 - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
 - Any sexually explicit content
- 5.1.6. Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- 5.1.7. Try to install any software or attempt to run unauthorised applications (games, scripts etc), all software required as part of your school work is pre-installed.
- 5.1.8. Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the IT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of Wolstanton High School's computers. This is illegal under the Computer Misuse Act.
- 5.1.9. Use or attempt to use Wolstanton High School's IT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- 5.1.10. Knowingly distribute or introduce a virus or harmful code onto Wolstanton High School's network or computers.
- 5.1.11. Copy, download or distribute any material from the internet or e-mail that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
- 5.1.12. Interfere with someone else's use of the IT facilities.
- 5.1.13. Be wasteful of IT resources, particularly printer ink, toner and paper.
- 5.1.14. Any attempt to gain access to restricted areas and;
- 5.1.15. Persistent attempts to circumvent the internet filter
- 5.2. If you are subjected to, or know about harassment or bullying, you are encouraged to report this immediately.

6. Implementation of the policy

- 6.1. Email messages sent are recorded and monitored.

- 6.2. Use of Wolstanton High School's internet connection is recorded and monitored.
- 6.3. The Network Manager checks computer logs on Wolstanton High School's network regularly.
- 6.4. Unsuccessful and successful log-ons are logged on every computer connected to Wolstanton High School's network.
- 6.5. Unsuccessful and successful software installations, security changes and items sent to the printer are also logged.
- 6.6. The Network Manager can remotely view or interact with any of the computers on Wolstanton High School's network. This may be used randomly to implement the IT Policy and to assist in any difficulties.
- 6.7. Wolstanton High School's network has anti-virus software installed with a centralised administration package; any virus found is logged to this package.
- 6.8. Users are required to be familiar with the requirements of the Data Protection Act 1998, and to ensure that they operate in accordance with the requirements of the Act. The obligations under the Act are complex but employees must adhere to the following rules:
 - Do not disclose any material about a person, including a pupil, without their permission
 - Such material includes information about a person's racial or ethnic origin, sex life, political beliefs, physical or mental health, trade union membership, religious beliefs, financial matters and criminal offences
 - Do not send any personal data outside the UK

7. Backups

- 7.1. Any data stored in your "my documents" area on the school computer is regularly backed up, if you lose any work please see the Network Manager.

8. Remote Access

- 8.1. Accessing the school resources such as network, devices or software from home the ICT Policy you have signed still applies.
- 8.2. Do not leave your computer unattended when still logged onto the school resources.

9. Email use

- 9.1. Students are responsible for all email sent from their account
- 9.2. Students should use only appropriate language and tone when sending emails
- 9.3. Students should not email large groups of users.

- 9.4. Students should not forward any spam emails
- 9.5. You must not try and exceed any access rights to systems or limitations on the use of data granted to you by the Network Manager.
- 9.6. Students are allowed to use USB Pens to transfer work to and from school, USB pens are not to be used to run any programs or games of any type.
- 9.7. Students should not store their work on the USB Pen as this is not backed up, students should use their “my documents” or onedrive as these areas is backed up regularly.

10. General IT Information

- 10.1. Emails and documents should be regularly checked and if no longer needed, deleted.
- 10.2. You must not try and exceed any access rights to systems or limitations on the use of data granted to you by the Network Manager.
- 10.3. Students should not store their work on the USB Pen as this is not backed up, students should use their “my documents” as this is backed up regularly.