June 2016

The Bulmershe School
INSPIRING POTENTIAL, ACHIEVING TOGETHER

Acceptable Use of Internet Technology Policy

Revised June 2016

This policy applies to all students and staff of The Bulmershe School and to individuals granted access to the School's information technology resources, or using their own equipment in School.

1. General Principles

- Access to the computer network and the Internet must only be via the user's authorised account and password, which must not be disclosed to any other person or organisation.
- Use of the Internet is permitted and encouraged where such use is suitable for education and learning purposes.
- School e-mail accounts (@bulmershe.wokingham.sch.uk) Internet IDs and web pages should not be used for anything other than school-sanctioned communications.
- Use of Internet/intranet and e-mail may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.
- The distribution of any information through the Internet, computer-based services, e-mail, and messaging systems is subject to scrutiny of the school. The school reserves the right to determine the suitability of this information.
- The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately.

Individuals must not:

- Use information technology for the purposes of deliberately upsetting anyone else within the school community (known as cyberbullying). This will apply outside of school as well as within, and on the user's own equipment as well as the School's.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access The Bulmershe School IT systems.
- Leave their password unprotected (for example written down)
- Perform any unauthorised changes or reconfiguration to IT systems.
- Attempt to access data that they are not authorised to use or access.
- Connect any non authorised device to the school's IT Network without prior approval of the Network Manager.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.

2. Internet and email Conditions of Use

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Visit Internet sites that contain obscene, hateful or other objectionable materials except in cases where they are required to do so as part of an investigation of an alleged breach of school policy. Under such circumstances, any viewing of obscene, hateful or other objectionable material must be conducted in the presence of a witness as appointed by the e-safety office or a member of the Executive Team.
- Use profanity, obscenities, or derogatory remarks in communications.
- Make use of public chat rooms.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the internet or email to represent personal opinions as those of the school.
- Place any information on the Internet that relates to The Bulmershe School, alter any information about it, or express any opinion about The Bulmershe School, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Send or forward anonymous messages, chain letters and spam (junk mail).
- Make official commitments through the internet or email on behalf of The Bulmershe School unless authorised to do so.
- Download any software without prior approval of the IT Network Manager.

3. Confidentiality

In order to reduce the risk of unauthorised access or loss of information, The Bulmershe School enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Individuals must not:

- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of school, or the school itself.
- Reveal or publicise confidential or proprietary information which includes, but is not limited to: financial information, databases and the information contained therein (e.g. Personal Information), computer software source codes, computer/network access codes.

4. Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only The Bulmershe School authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

5. Software

Employees must use only software that is authorised by The Bulmershe School on The Bulmershe School computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on The Bulmershe School computers must be approved and installed by The Bulmershe School IT Department.

6. Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within The Bulmershe School. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Bulmershe School anti-virus software and procedures.

7. Non-Conformance to the Acceptable Use Policy

Not abiding to this Acceptable Use Policy may result in denial of some or all of the school's IT systems, along with disciplinary action in line with the School's Procedures and Policies.

Any Illegal actions may be reported to the proper authorities.

8. Liability

The Bulmershe School has no expectation that personal IT equipment will be used. The Bulmershe School Governing Body accepts no responsibility for loss or damage to individuals personal equipment.

9. Telephony (Voice) Equipment Conditions of Use

Use of Bulmershe School voice equipment is intended for business use. Individuals must not use Bulmershe School voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

10. Monitoring and Filtering

All data that is created and stored on The Bulmershe School computers is the property of The Bulmershe School and there is no official provision for individual data privacy, however wherever possible The Bulmershe School will avoid opening personal emails. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The Bulmershe School has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

11. Reference Information

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 1998
- The Bulmershe School e-Safety Policy
- The Bulmershe School Data Protection Policy

It is your responsibility to report suspected breaches of security policy without delay to your line management and the IT department.

All breaches of information security policies will be investigated. Where an investigation reveals misconduct, disciplinary action may follow in line with The Bulmershe School disciplinary procedures.