The Stourport High School & VIth Form College

Acceptable Use Policy

(Acceptable Use of Electronic Communications Policy including ICT Network Use & Data)

1. Introduction

The Acceptable Use Policy applies to members of staff or contract staff that are employed by The Stourport High School & VIth Form College who need to access the network. The Acceptable Use Policy also applies to school owned equipment which is not connected to the network.

Responsibility for updates and the maintenance of the Acceptable Use Policy rests with the School Business Manager who is in charge of ICT.

Policy Statement:

The school provides PCs, laptops, tablets and handheld computers (PDA) together with access to e-mail and the Internet and encourages their use wherever it assists job performance. The Acceptable Use Policy applies to all users of the school's PCs, laptops, tablets and PDAs, as well as everyone who has access to the school's network, including employees, agency staff or contractors. The Acceptable Use Policy applies to the school's ICT systems, hardware and software, also to the 'word' whether spoken or transmitted electronically via e-mail and content transmitted across any such system.

The school has a number of legislative requirements that must be adhered to in relation to the IT network and any specific applications, e-mail and Internet use. The Acceptable Use Policy defines for all staff what is 'acceptable' and 'unacceptable' use of the school's systems.

The Acceptable Use Policy (AUP) is important to make staff fully aware of what constitutes misuse.

This AUP supersedes all others and applies to staff only.

2. Risks to the School & Legal Requirements

2.1 Risks to the School

Whilst use of e-mail and the Internet in particular is often essential for job performance, it can expose the individual and the school to the risk of a legal claim including:

- a defamation claim;
- a discrimination claim, whether on the grounds of gender, race, disability, sexual orientation, religion or age;
- a harassment or use of offensive language claim;
- a breach of copyright claim;
- a breach of contract claim;
- a claim for breach of the duty of confidentiality;
- a criminal prosecution following the discovery of child pornography or unlicensed software (such as books, films or music) on the network;

- a criminal prosecution or civil action following a breach of data protection legislation.

It is for this reason that the school needs to set out in this Acceptable Use Policy clear rules for use of its systems, the consequences of misuse and the measures the school will take to monitor compliance with the Acceptable Use Policy.

Guiding Principle:

If a member of staff is in any way unsure or unclear whether their use of the school's ICT facilities and equipment could be deemed as inappropriate or likely to lead to a claim of misconduct, they should discuss their concerns with their Line Manager before using the system.

2.2 Legal Requirements

The following legal requirements have been considered in the formation of the Acceptable Use Policy.

Data Protection Act 1998	Messages containing personal information, personal opinions about an individual or the opinions of an individual are all covered under the Act. Advice suggests that the risk of not monitoring illegal content, time wasting by employees, breach of copyright and defamation outweighs the entitlement to privacy under the *Human Rights Act*. In order to comply with the law, any monitoring that is undertaken must follow the procedures outlined in the Acceptable Use Policy.
Human Rights Act 1998	Under *Article 8* of the *Human Rights Act* 'everyone has a right to respect for his private and family life, his home and his correspondence'.
Freedom of Information Act 2000	All e-mail falls within the scope of the *Freedom of Information Act*.
Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice (Interception of Communications) Regulations 2000	All interception must be authorised and there must be mutual consent and good business reason for doing so. Includes access to e-mails before they have been opened by the intended recipient, however does not include items opened and stored.
Defamation Act 2013	E-mail can contain defamation and it circulates very quickly. Due to the broadcasting capabilities of e-mail, defamatory comments are likely to be treated as 'libel' and therefore there is no requirement to prove damage.

3. Use of School ICT Systems

At all times users must comply with the law in their use of the school's ICT equipment and systems. Examples of inappropriate activities include, yet are not limited to, examples quoted in this section of the Acceptable Use Policy.

3.1 IT Network & Applications

The school is at risk from virus attack and loss of reputation caused by unprofessional work practices. To minimise these threats users should not:

- install or download non-business related software, ICT Support can advise on this;
- connect a PC or laptop which is not school property and which has not been already connected to the network by ICT Support;
- store data about individuals on the system unless the storage is covered by the school's data protection registration under the *Data Protection Act 1998*;
- fail to comply with the school's Password Guidance (for example: passwords should be made up of a mixture of capital and lower case letters and numbers; users should not allow another user access to their password or leave a work station unlocked);
- engage in criminal activity, for example fraud.

3.2 Internet

Users should not:

- visit, view or download any non-job-related material from any Internet site, which contains illegal material (such as child pornography, obscene material or race hate) or other inappropriate material. Examples of inappropriate material include, however are not limited to, criminal skills, terrorism, cults, gambling, illegal drugs and pornography;
- copy or modify copyright protected material downloaded from the Internet without authorisation;
- use the Internet for criminal activity, for example, yet not limited to, software, film/video and music piracy or the sale of illegal goods.
- access unauthorised instant messaging sites of any kind.

3.3 E-mail

Users should:

- adopt a responsible approach to the content of e-mails, bearing in mind that e-mails often need to be as formal as any other form of written correspondence, such as a letter;
- be aware that e-mails are disclosable in any legal action against the school and e-mails, which have been deleted by a user or from the network, may be recovered;
- remember that e-mail correspondence is not private, as e-mails can be easily copied, forwarded or archived without the original sender's knowledge. When

drafting any e-mail, a user should bear in mind that it may be read by a person other than the designated recipient;

- consider whether e-mail is the most appropriate way of communicating the message, particularly when dealing with sensitive matters or where debate is likely.

Users should not:

- send an e-mail message which is abusive, malicious, discriminatory, defamatory or libellous about any person or organisation, or which contains illegal, obscene or offensive material. Before sending or forwarding any e-mail staff should ask themselves if they can support their actions in a disciplinary hearing or in court. It is recommended that a member of staff inform their Line Manager if they receive such a message;
- send e-mail which could be deemed as bullying or harassment;
- send information externally which may infringe the intellectual property rights of a person or organisation;
- open attachments or e-mails from unknown sources if they appear suspicious;
- forward 'chain mail', unsolicited bulk e-mail messages or "spam".

3.4 Electronic Communication with Students

All staff must ensure that electronic communication with students is:

- always conducted via the schools Outlook e-mail account or through the 'shsapps.co.uk' secure Google Apps domain;
- never conducted via social networking sites or texts;
- strictly business-like and factual avoiding informal tones, vocabulary and/or topics;
- reported immediately to the Executive Principal (or Associate Principals in the Executive Principal's absence) in the event of any apparently inappropriate electronic communication by any party.

3.5 Personal Use

Occasional personal usage is a privilege and can be withdrawn if abused. The school tolerates limited personal use of its equipment and the network provided that the following conditions are met:

- all personal usage is kept short; excessive time is not spent sending personal e-mail or surfing the Internet for non-work-related purposes. The test of what is acceptable personal use is that there should be no interference with the performance of the user's work commitments or with business use of the network. The presumption is that this activity will principally take place in the user's own time;
- that e-mail messages do not constitute misuse according to the rules outlined in the Acceptable Use Policy.

If excessive personal use is suspected, then the expectation is that the Line Manager would speak to the individual and set more specific parameters. Line

Managers would be permitted to prevent all personal use if the parameters were not respected.

Users must not have an expectation of privacy when using the school network as all use may be monitored. If a user wishes to ensure the privacy of any information, for example when communicating with the Personnel Services or with a trade union representative, he/she should not use e-mail and use the internal post instead.

3.6 Disciplinary

Breach of the regulations referred to in this section may result in disciplinary action being taken against an employee up to and including dismissal. Any action against the employee will follow the school's disciplinary procedures. Specific analysis of individual e-mail messages or network use will be provided in support of any investigation.

A breach of the regulations or this Acceptable Use Policy in any way by a user who is not an employee may result in legal action being taken against the user.

3.7 Password Security

Each user gains access to the network by setting their own unique password, which must be at least six characters long and should be changed regularly. Best security practice is that password details should not be shared with any other user and each user is responsible for managing their own password.

More detailed guidance can be obtained from ICT Support.

4. Monitoring & Reporting of Network Use

Monitoring describes processes that take place automatically whereby information is retained by ICT Support in order to maintain an audit trail of activity on the network. Reporting describes the extraction of data relating to individual use for the purposes of investigation.

4.1 Monitoring & Recording of Communications

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("the Regulations") enable designated staff to carry out interception of employee's communications using the school's systems for the purposes briefly described below:

- recording the evidence of business transactions (e.g. establish facts);
- ensuring compliance with regulatory or self-regulatory guidelines;
- maintaining effective operation of the school's systems (e.g. preventing viruses);
- monitoring standards of training and service;
- preventing or detecting criminal activity;
- preventing unauthorised use of the computer system i.e. ensuring that the employee does not breach this or related school policies.

The school will only do this solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the school's activities which pass through the school's own systems.

All employees should take note that every person who uses the school's systems to send or receive information may have their communications intercepted.

4.2 How we will monitor & if necessary record?

The school fully appreciates that employees have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy whilst in the work environment.

Any monitoring will be carried out subject to the requirements of legislation including the *Data Protection Act 1998*, the *Human Rights Act 1998*, the *Freedom of Information Act 2000*, the *Regulation of Investigatory Powers Act 2000* and the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*.

Network traffic and the performance of the network will be monitored and the school will use a firewall, anti-virus products, intrusion detection and prevention systems and other software to do so.

Specific monitoring of information will be undertaken as follows:

- anti-virus software will monitor all communication, however will only record and quarantine those which it identifies as containing a virus;
- software may monitor e-mail content by searching for key words. A log will be kept for 12 months of e-mails which are picked up following such monitoring;
- software will prevent access to certain designated non work-related Internet sites. A record will be maintained of sites visited and sites which users have attempted to visit;
- spot checks may be made on the communications of individuals or groups on a random basis to ensure the Acceptable Use Policy is being applied with.

The monitoring above is confined to monitoring traffic data and where appropriate recording it rather than the contents of communications. The content of communications will only be examined and reported on if it appears there may have been a breach of the law or of the school's policies or procedures. Personal information collected through monitoring, for purposes other than those for which the monitoring was introduced, will not be used unless:

(a) it is clearly in the employees' interest to do so; or

(b) it reveals activity that no employer could be reasonably expected to ignore.

If no further action is to be taken as a result of the report, the content will be destroyed as soon as that decision is made. If further action is taken as a result of a report, then the data will be stored in accordance with the retention schedules for disciplinary matters.

4.3 Incident Reporting

It is intended that this guidance note and associated reporting of incidents (which is set out in more detail in the AUP Appendix 1 (below)) will be used by all staff and managers who are involved in an incident or have one reported to them.

In the interests of all school staff they are to report all incidents of misuse with as much information as possible and for these to be investigated as thoroughly as possible.

5. Remote Use

Users will sometimes need to use school equipment and access the school network when working remotely, whether from their home, off-site or when travelling. Remote users are reminded that this Acceptable Use Policy applies to them wherever they are using school owned equipment and/or accessing the school network. Users should be particularly careful to secure access to the network by using their password when working from home, in hotels or on public transport.

Users should not:

- allow members of their family or anyone else to use the school network or school equipment;
- display confidential information on the screen of their computer at any time where it may be visible to a non-school employee;
- leave hardware in vulnerable locations such as cars, etc.

6. e-Safety

- We recognise our responsibility to educate students regularly regarding e-Safety, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies. This takes place in ICT/Computer Science lessons, SMSC days, PDWB sessions and assemblies.
- All members of staff receive regular updates regarding e-Safety with regard to recognising and reporting concerns.

7. Misconduct

Compliance with the Acceptable Use Policy will be audited and for the avoidance of any doubt on the part of employees or managers, this section explains conduct or behaviour that would be deemed as 'unacceptable' use. Any breach could be deemed as serious or gross misconduct.

Examples of misconduct may include, yet is not limited to:

- sending written or verbal abusive, offensive, illegal or defamatory messages or material;
- sending written or verbal messages which could constitute harassment or bullying;
- excessive personal use of e-mail or the Internet in work time;
- introducing a virus to the system by inserting a disk or memory stick into a school PC or laptop without running a virus check, via e-mail or from downloading an Internet file;
- misuse of e-mail, the Internet or the system generally which results in a legal claim being made against the school;

- accessing illegal material or pornography on the Internet;
- unauthorised downloading and distribution of software or files;
- accessing proxy sites or other methods to bypass systems put in place to protect the school network;
- use of the Internet for criminal activity;
- hacking, or other breaches of the *Computer Misuse Act 1990*.

8. General

This Acceptable Use Policy may be amended at any time and any changes will be notified to users.

Users of the school's network will be expected to have read and understood this Acceptable Use Policy.

Contact Details:

School Business Manager in charge of ICT, The Stourport High School & VIth Form College, Minster Road, Stourport-on-Severn, Worcestershire, DY13 8AX.

Managers Guidance Relating to an Investigation

Managers are advised to discuss reporting with Legal and Personnel prior to any investigation taking place.

Producing a report may involve having access to personal information about other workers, particularly when it extends to e-mail. As far as possible, such information should be excluded from the report and where this is not possible the number of people who have access to the information should be kept to a minimum. Legal advice should be obtained to ensure that data protection principles are not breached.

Covert reporting can only be justified if openness would be likely to prejudice the prevention or detection of crime or serious malpractice. The covert watching of another person is not in itself subject to the Data Protection Act; however, once it results in a record being kept about the worker, the Act will apply. Under the *Regulation of Investigatory Powers Act (2000)* and the *Telecommunications (Lawful Business Practice (Interception of Communications) Regulations 2000*, interception of an unopened e-mail without consent is only permissible under very specific circumstances. Managers must seek legal advice if they plan to intercept e-mail(s) without consent.

The evidence will then be considered and appropriate action taken.

The Stourport High School & VIth Form College

Acceptable Use Policy - Appendix 2

****** Please print off this page only ******

Staff Agreement Reply Form

Acceptable Use Policy

Acceptable Use of Electronic Communications Policy including ICT Network Use & Data

To: Ms Lorna Deakin, Principal

Print Name: ....

Date: ....

I have read and agree to follow the Acceptable Use Policy.

Signed: ....

Please print, date and sign, then return form to the School Business Manager in the Admin Hub.

If, for any reason, you do not agree with the Acceptable Use Policy, please note below the details and return to the School Business Manager.