ACCEPTABLE USE POLICY [01-0064]

1 Introduction

This Acceptable Use Policy document stipulates constraints of practices to which all users must agree prior to gaining access to the College's digital resources including hardware, network or internet. All users must read, understand and agree to this policy before they access any digital systems.

This Acceptable Use Policy sets out the ways in which the College's digital systems are to be used.

Halesowen College provides network facilities for all College staff, students and governors for use in support of their employment/learning. Halesowen College is part of the Joint Academic Network (JANET) which is a collection of networking services and facilities which support the communication requirements of the UK education and research community) and as such must comply with the conditions of the JANET Acceptable Use Policy which can be found on their website www.ja.net.

The acceptable use rules are in place to protect the individual and the College. Inappropriate use exposes Halesowen College to risks including virus attacks, compromise of systems/ services, failure to uphold our safeguarding duty and legal issues. Failure to adhere to this policy may lead to disciplinary action in accordance with College policies.

The College reserves the right to exercise control over all uses of its digital and information facilities, including examining the content of users' data as permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000:

- For the proper regulation of the College's facilities;
- To ensure compliance with this Acceptable Use Policy;
- In connection with properly authorised investigations in relation to breaches or alleged breaches of provisions in the College's regulations;
- To meet legal requirements;
- To protect the network against viruses and other malicious content.

Any reasonable action may be taken to protect the network, its users and its services.

2 Policy Remit

This Acceptable Use Policy affects all eligible users of computer facilities provided by Halesowen College. Eligible users are defined as:

- All employees, governors and volunteers (herein referred to as staff);
- All enrolled students ;

- Potential students attending taster or introductory sessions;
- Recognised Trade Unions;
- Visitors and contractors;
- Any other users as may be defined from time to time depending on College activities.

When using privately owned equipment and accessing College resources, or accessing the internet and other digital services through the College infrastructure, the conditions of this Acceptable Use Policy apply.

3 Access Controls

The College systems are controlled by the use of user ID and passwords, and may only be accessed and used with prior authorisation by the College. Authorisation is specific to an individual. All user IDs and passwords are uniquely assigned to named individuals and as such, users are accountable for all their actions on College systems.

Users must **not**

- allow anyone else to use their ID and password;
- leave their user accounts logged in at an unattended and unlocked computer/mobile device;
- use someone else's user ID and password;
- leave their password unprotected (for example writing it down);
- perform any unauthorised changes to IT systems or information;
- attempt to access data that they are not authorised to use or access;
- access data for a purpose other than that which they are authorised to do;
- exceed the limits of their authorisation to interrogate the systems or data;
- connect any non-authorised device to the network or IT systems;
- store data on any non-authorised equipment;
- give or transfer data or software to any person or organisation within the authority of Halesowen College.

Compliance with this policy is part of the student learning agreement and the staff code of conduct.

4 Viruses and Virus Checking

The College will take all reasonable steps to ensure that suitable security and virus checking software is in place and updated regularly. Centralised automated virus detection is in place. All College owned devices have anti-virus software installed.

Users have a responsibility not to compromise the security of the network. To minimise the risk of virus infection, users must follow the Safe Computing Guidelines (see Appendix B of this policy).

5 Access to and Use of the Internet

Use of the internet and email is primarily intended for staff business use, and learning activities for students. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Halesowen College in any way, not in breach of any terms and conditions of employment and does not place the individual or Halesowen College in breach of statutory or other legal obligations.

All individuals are accountable for their actions on all digital systems.

Individuals must not

- use the internet, email, Buzz et al for the purposes of harassment or abuse;
- use profanity, obscenities, or derogatory remarks in communications;
- access, download, send or receive any data (including images), which Halesowen College considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material;
- use internet, email et al to promote radical ideas/concepts;
- introduce malicious programmes eg viruses, worms, email bombs etc;
- commit any criminal offence (knowingly or unknowingly);
- use the internet or email to make personal gains or conduct a personal business;
- use the internet or email to gamble;
- make fraudulent offers of products, items or services;
- use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam;
- make official commitments through the internet or email on behalf of Halesowen College unless authorised to do so;
- download copyrighted material which may include but is not limited to music media, film and video files;
- in any way infringe copyright, database rights, trademarks or other intellectual property;
- download any software from the internet without prior approval of the infrastructure team;
- connect Halesowen College devices to the internet using non-standard connections;
- breach the Data Protection Act;
- circumvent user authentication or security of any host, network or account;
- personal use must not be during times when the user should be engaged on College activities.

In using digital communication, users must apply the same values and principles that apply to other forms of communication on behalf of the College. It is the user's responsibility to discourage friends and colleagues from outside of the College from sending such material. It is recognised that some unacceptable material may be sent unsolicited, this should be reported to the relevant line manager. Users should check College email accounts at least once a day and keep mailboxes tidy.

Use of social networking sites and blogs is subject to the College's Social Media Policy. Blogging and vlogging are also subject to the terms and restrictions set out in this policy. They are acceptable providing it is conducted professionally and responsibly and not detrimental to Halesowen College not interfering with an employees work duties.

In line with the clause on reasonable personal use, the use of any Halesowen College equipment for the playing of games, or any software deemed a game, is not prohibited provided that it is appropriate (eg during lunchtime and breaks), does not affect the availability of resources to other users and does not violate the policy in any other way.

All use of such facilities will be monitored.

Software and computer-readable datasets made available on the College network may only be used subject to the relevant licensing conditions. Users must not install any software onto College computers without specific authorisation. The unauthorised use and copying of software is illegal. Software may be used only for the purposes defined in the licensing agreement and on computer systems covered by that agreement. Copies of the various licensing agreements are held by the Technical Resources Manager who will advise users as appropriate.

6 The Data Protection Act and other Relevant Legislation

Users are required to comply with the College Data Protection Policy and the Data Protection Act.

Other relevant legislation includes

- The Computer Misuse Act
- The Copyright, Designs and Patents Act
- Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Intellectual Property Act 2014

7 Security of Computing Equipment and Data

- Portable devices must be kept securely. They should ideally be secured with a Kensington type lock or locked in a drawer or cabinet when left unattended. Users should exercise judgement over the security of portable equipment left in offices.
- Any loss, theft of, or damage to IT equipment must be reported immediately to the Director of Finance and Corporate Services.
- No non-mobile equipment should be removed from College sites unless the appropriate loan forms have been completed.
- All rooms should be locked when unoccupied.
- Mobile storage devices must only be used when network connectivity is unavailable or there is no other appropriate method of transferred data. When storing sensitive or confidential data encryption enabled must be used.
- Data stored in approved areas will be backed up automatically eg staff O: drives, student H: drives.
- Data stored in other areas will not be backed up (eg on local C: or D: drives of PCs), and no attempt will be made to recover it in the event of any loss.

- Hard drives of student and shared staff machines may be re-imaged at any time and no responsibility will be accepted for loss of any data stored on them.
- Every reasonable effort will be made to provide backups of all data in approved areas, but no responsibility can be accepted for any data loss caused by failure of hardware or software.

8 Telephony

Use of Halesowen College voice equipment is intended for business use. Individuals must not use voice facilities for sending or receiving private communications on personal matters, except in accordance with the approved policy on private calls.

Individuals must not

- use Halesowen College voice equipment for conducting private business;
- make hoax or threatening calls to internal or external destinations;
- accept reverse charge calls domestic or international operations, unless it is for business use.

9 Actions upon Termination of Contract

All Halesowen College equipment must be returned to Halesowen College at termination of contract for staff and on completion of the course for students.

All Halesowen College data or intellectual property developed or gained during the period of employment remains the property of Halesowen College and must not be retained beyond termination or reused for any other purpose.

10 Unacceptable Use

College information systems cannot be used for any activity that may reasonably be regarded as unlawful or potentially so. This includes but is not limited to

- creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety;
- creation or transmission of material with the intent to defraud;
- creation or transmission of defamatory material;
- creation or transmission of material such that this infringes the copyright of another person(s);
- creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their organisation has chosen to subscribe.
- deliberate unauthorised access to networked facilities or services.

- deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:
  - wasting staff effort or resources
  - corrupting or destroying data
  - violating the privacy of users
  - disrupting the work of users
  - denying service to other users (for example, by overloading of access links or switching equipment of services
  - continuing to use an item of software or hardware after the Infrastructure Team have requested that use cease because it is causing disruption to the correct functioning of systems
  - other misuse such as the introduction of 'viruses' or other harmful software
  - reputational damage to the College
  - bullying, harassment of another individual
  - promotion of radical ideologies or contravention of British values
  - any criminal activity (refer to Incident Handling Procedure for Criminal Computer Misuse)

The College reserves the right to amend and update these conditions as necessary.

Any contravention of the above terms and conditions may lead to action in accordance with the College disciplinary procedures.

Offences by students will be subject to the Code of Student Discipline as set out in the Student Charter unless this is superseded by law.

The College encourages staff and students to make full and productive use of the facilities provided to them within the scope of acceptable use.

Review

Reviewed/Approved	**By**	**Date**
Updated by	Jacquie Carman	07.07.16
Approved at		

College Computer User's Agreement

All staff, governors, volunteers, students and any other user who has access to College digital systems are bound by the College Acceptable Use Policy.

Before you access College systems or resources you must indicate that you have read, understood and agree to comply with the Acceptable Use Policy. By logging on you have indicated your agreement to adhere to this Acceptable Use Policy.

Safe Computing Guidelines

Viruses

College equipment has virus protection which is updated automatically. However, there is still a risk of infection from viruses that are newer than the virus checker. Hundreds of new threats are discovered every week and it is impossible to warn against them all. To minimise the risk, users should always follow these guidelines.

- Whenever a new type of threat is discovered, information will be posted on the College staff hub as an announcement and/or Buzz as appropriate.
- Users should never assume that email attachments are safe simply because they have been sent by a trusted source. Many viruses forward themselves to everyone in an address book to make it look as if they have come from a trusted source.
- Users should never open any email attachments not related to College activities, including but not limited to, screen savers, executable files, pictures and movies.
- Users should never run any 'joke' programs, eg Xmas Lights. Virus infected versions of many normally harmless programs are circulating the Internet.
- Users should be wary of any executable file received from a mailing list and exercise caution when downloading from the internet.
- Whenever a problem is suspected with your virus checker, users must switch off and notify the IT Hotline immediately.
- If users have any suspicions at all about any file they should NOT open it but contact the IT Hotline for advice.

A virus infection on a single PC can quickly spread and seriously affect the entire network and other PCs on it. Users may be held responsible for any damage if they cause a virus outbreak as a result of breaching these guidelines.

Virus Hoaxes

- Virus hoaxes are emailed warnings about non-existent viruses which usually ask the user to forward them to everyone in the address book. These are designed to create hysteria and unnecessary load on email servers and networks.
- On receipt of any emailed warning about possible viruses, contact the IT hotline.

Phishing

- 'Phishing' is a practice used by fraudsters to trick people into revealing personal information such as credit card numbers and online banking passwords by sending an official looking email pretending to be from a legitimate organisation. The email will contain links which direct you to a copy of that organisation's website and will ask users to log in or enter other information.

- The emails usually use certain scare tactics to encourage users to follow the link to the site, for example saying there has been a security alert on your bank account or an unrecognised transaction on the user's credit card. Another common ploy is to send a failed delivery notification from a courier company such as FedEx and asking you to enter the user's personal information to reschedule the delivery.

- These emails are sent at random, so it is not unusual to receive an email from a bank that users do not have an account with.

- If any suspicious emails are received users must NOT follow any links, no matter how urgent the email makes the matter sound. In accordance with the Anti-Fraud Policy, should any employee receive a scam email to their College email these should not be opened but forwarded to the IT and Systems Director who, in liaison with the Director of Finance and Corporate Services or College Accountant, will report these to Action Fraud: www.actionfraud.police.uk. Even though no money may have been lost reporting to Action Fraud enables crucial intelligence to be gathered and preventative action taken. If the email is received in a College email account, please forward it to postmaster@halesowen.ac.uk for advice. If the email is received in a personal account then users may wish to forward it to the organisation it claims to be from so they can carry out their own investigation.

- Genuine organisations will usually make an effort to prove their authenticity by including the user's name or part of your address in the message. Fraudulent emails often have poor spelling or grammar.

- Banks and other organisations will use other means than email to contact users if there is an urgent problem with their account - users should not be panicked into giving away logon details.

Cyber Bullying and E-Safety

Cyber bullying is not tolerated at Halesowen College. In furtherance of the duty to safeguard learners the College will take all reasonable measures to ensure students and staff stay e-safe.

Cyber bullying can include:

- Sending or posting cruel messages or images;
- Threatening others;
- Excluding or attempting to exclude others from activities;
- Starting or passing on rumours about others;
- Harassing or intimidating others;
- Sending angry, rude or vulgar messages directed at a person or persons privately or to an online group;
- Sending or posting harmful, untrue or hurtful statements about a person to others;
- Pretending to be someone else and sending or posting material that makes that person look bad or places that person in potential danger;
- Sending or posting material about a person that contains sensitive, private or embarrassing information, including forwarding private messages or images; and/or,
- Engaging in tricks to solicit embarrassing information that is then made public.

E-safety applies to the use of all digital communication devices such as email, mobile phones, game consoles and social networking.

Users will be asked to remove material from any service that contravenes these guidelines, even if it was not posted using College facilities and the user may be subject to College disciplinary procedures.

If students become aware of activity that may contravene the guidelines they should report it to their personal coach. Staff should express concerns to their line manager in the first instance. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and action taken in line with staff and student disciplinary policies.

E-safety is reviewed and maintained by the Health and Safeguarding Forum. Students will be made aware of e-safety through the tutorial curriculum, and training will be provided for staff as appropriate. Staff should be a model example to students at all times.

Associated policies and procedures:

- Safeguarding Policy
- Code of Conduct
- Criminal Computer Misuse