Communication and Acceptable Use Policy

Wistaston Academy
Primary and Nursery School
Together We Learn • Together We Achieve

Policy Author	Linda Davis
Responsible Governor's Committee	Finance, HR and Resources
Date discussed at SLT Meeting	19.04.17
Date discussed at Staff Consultation Committee	22.03.17 21.04.17
Date discussed at Staff Meeting / Morning Briefing	26.04.17
Date established and approved by Governors	Summer 2015
Frequency of Review	Review in the light of changes to legislation or operating experience
Website	No

Wistaston Academy Policy Statement:

Electronic communications resources must only be used for conducting the business of and/ or furthering the business interests of Wistaston Academy unless authorised by the Principal.

Purpose

Wistaston Academy aims to encourage the maximum positive use of ICT within the school in order to enhance teaching, learning, attainment, administration, management and efficiency. The school is committed to the delivery of a high quality ICT provision within a safe environment.

The policy for the Acceptable Use of ICT has been produced to ensure protection of all parties – the pupils, the parents, the staff and the School. The school reserves the right to monitor, view or delete any data that may be held on its computer systems and to monitor network, internet and email use.

The purpose of the document is to establish guidelines as to what constitutes 'computer and telephony resources' what is considered to be 'misuse' and how users should operate within a clear desk environment.

The misuse of Wistaston Academy's computer and telephony resources is considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action including dismissal.

The policy has been developed to advise employees of if, when and under what conditions they may use Wistaston Academy's communications and information systems for personal use. It sets standards to ensure that employees understand the position and do not inadvertently use communications and information in inappropriate circumstances.

Wistaston Academy recognises employees' rights to privacy but needs to balance this with the requirement on the School (as a public service) to act appropriately, with probity, to safeguard its business systems, and to be seen to be doing so.

In applying the policy, the School will act in accordance with the Human Rights Act 1998 and other relevant legislation and will recognise the need of employees to maintain work/life balance.

Scope

This policy covers all forms of communication, information retrieval (from any source), media and equipment, used for official business and regardless of origin, ownership or place of use, for example:

- mail systems (internal and external)
- internet and intranet (email, web access and video conferencing)
- telephones (hard wired and mobile)
- pagers
- fax equipment
- computers
- photocopying, printing and reproduction equipment
- recording / playback equipment
- documents and publications (any type or format)

The policy applies to all employees (as a contractual term), agency staff and to other people acting in a similar capacity to an employee. It will also apply to staff of Contractors and other individuals providing services/support to the Council (e.g. volunteers). It takes account of the requirements and expectations of all relevant legislation.

Managers will discuss the policy with their teams and agree parameters within which team members will act. This will take into account for example, whether or not there is a public phone in the building, whether or not employees are able to leave the premises during break periods, etc, and should be in writing. Every employee will have the policy explained to them at induction, and be given a copy for future reference. If at any stage employees require further clarification, they should speak to their manager in the first instance.

Where an employee needs to discuss personal information with Occupational Health, Personnel or their Trade Union, they will be given privacy to do this.

Managers will agree with Trade Union representatives the arrangements for using school communication and information systems which will be provided in accordance with trade union facilities agreement and the ACAS Code of Practice.

Use of equipment and materials

It is expected that staff must not carry out personal activities during working hours, nor mix private business with official duties. Official equipment and materials should not be used for general private purposes without prior permission from an appropriate line manager. This will usually be in writing or may be covered by the parameters agreed by the manager.

Facilities for Private Use

In terms of using Wistaston Academy equipment and materials, the decision to allow such use is at the Manager's discretion. However the following are provided as examples to illustrate where it might be reasonable for permission to be given for reasonable use for private purposes, under the conditions shown and after getting prior approval, in writing if this is required. A senior manager may veto private use at any time if they consider that circumstances justify this in general or particular cases, e.g. because of improper use or over-use. A charge may be made for materials if the values are significant.

- Social or recreational activities associated with School employment.
- Regular activity for a legitimate voluntary body or charity - but prior written approval from a senior manager must be obtained.
- Training or development associated with School employment.
- Occasional and brief essential family communications or other personal messages. In emergencies permission might need to be obtained retrospectively or again this may be covered by the general parameters agreed with the manager.

If given permission, approved acceptable private use should normally take place in the employee's own time but where this is not practicable or sensible, any disruption to the employee's official work or that of colleagues must be minimal. Official work will always take precedence.

All uses, whether for private or official purposes, must observe:

- the law
- Financial Regulations and Codes of Practice on Financial Management
- Terms of employment, especially the Code of Conduct for Employees
- Communications & Information Technology (ICT) Code of Practice

It is not acceptable to use Academy equipment and materials or an employee's own equipment/materials in the workplace in any of the following contexts:

- Illegal activity.
- Activities for private gain.
- Personal shopping.
- Excessive personal messages.
- Playing games.*
- Gambling.
- Political comment or any campaigning.
- Personal communications to the media.
- Use of words or visual images that are offensive, distasteful or sexually explicit.
- Insulting, offensive malicious or defamatory messages or behaviour.
- Harassment or bullying
- Random searching of the web.
- Accessing sites which could be regarded as sexually explicit pornographic or otherwise distasteful or offensive.
- Using message encryption or anonymised web search, except where encryption is required for official School business purposes.

- Racist, sexist or other conduct or messages which contravene the Council's employment diversity policies.
- Actions which could embarrass the Council or bring it into disrepute.

*except those games pre-loaded as part of the Microsoft programme suite, which may be accessed in the employee's own time.

No exhaustive list can be prepared defining all possible forms of misuse of computer resources. The individual circumstances of each case would need to be taken into account.

Inadvertent access to inappropriate sites and inappropriate emails

If an employee inadvertently accesses an inappropriate web site, they should leave it immediately but notify their manager of the incident, giving the date and time, web address (or general description) of site and the action taken. This will help safeguard their position in circumstances where disciplinary action would otherwise result.

Employees may find themselves receiving emails which contravene this policy. In the case of comparatively innocuous material (e.g. 'clean jokes'), the recipient should point out to the sender that they do not wish to receive such messages at their workplace because they believe they contravene the Council's policy. If there is repetition, the employee should retain the messages and notify their manager. If the emails are racist or sexist or could otherwise be regarded as offensive, they should be left in the inbox and the manager notified immediately. Employees should notify the sender that they do not wish to receive further such material and keep a record of doing so.

Monitoring

Monitoring information will not be accessible (or distributed) any more widely than is necessary for the purposes for which it is needed.

All employees should be made aware at induction and at intervals thereafter in relation to any electronic communication, there can be no expectation of absolute privacy when using School equipment provided for official/ work purposes; and that the School reserves the right to monitor all communications including their content. This monitoring is carried out to ensure that equipment and systems are used efficiently and effectively, to maintain systems security and to detect any breaches of this policy or the law. Normally monitoring consists of the following:

- **Telephones and fax.** An automatic record is kept of every number called, from where and the duration of the call. Further action is taken where particular numbers called or the frequency and duration of calls suggest abuse of this policy. The School reserves the right to monitor communication content selectively if abuse is suggested. However such monitoring would only take place following an assessment that such steps are necessary to further a particular investigation or concern.

Telephone response times will be sampled from time to time.

- **Emails.** Every incoming and outgoing email message is automatically swept for key words which could indicate misuse.

- **Web access.** Access to some web sites is automatically prevented (e.g. pornographic, racist and violent sites) and others are restricted (e.g. MP3 music sites and Web Chat) and a message warns that these types of sites are strictly for business purposes. However, an automatic record is made of all sites visited and a sweep made of site names and content against pre-determined criteria, to identify inappropriate sites together with attempts made to access such sites.

- **Mail.** The privacy of internal and external postal communications marked 'personal' will normally be respected (unless abuse of this policy is suspected) but all other communications may be opened for good reason by a manager, secretary or colleague.
- **Telephone.** Wistaston Academy has a practice of acceptable use relating to telephone use. Personal calls made/received must not be excessive and must not interfere with business use.

Access to and retention of monitoring information

Access to routine monitoring information is restricted to specified employees in Information & Communication Technology Services and Audit. Regular reports will be produced identifying high usage of communications and information technology and areas where the School may be at risk, e.g. as a result of weak passwords. These will be made available to managers. If the manager identifies a potential issue of abuse they will be given access to more detailed information to enable them to decide whether further investigation is necessary and enable appropriate action to be taken. They will respect the confidentiality of all communications and

disclose the contents of communications only where there are grounds for suspecting abuse of this policy. Where this is the case, other senior managers may then be involved and are likely to be made aware of the contents of communications.

Risks

Wistaston Academy recognises that there are risks associated with users accessing and handling information in order to conduct official School business.

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies without the correct authorisation and clearance may unintentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and an inability to provide necessary services.

Surveillance

Permanently fitted surveillance cameras are installed at the school only for security and safety reasons and will always be visible to people within their range. Video recording tapes will be kept secure, the information used only for security purposes. No automatic connections will be made between information from security cameras and other monitoring sources.

Security

Every employee must observe the School's communications and information technology security requirements (as detailed in the ICT Code of Practice) and act responsibly when using equipment and materials. Managers will take the most serious view of any action or inaction on the part of an employee who deliberately, recklessly or carelessly jeopardises the security of records or systems. Any employee detecting a potential security problem (e.g. a virus or unauthorised access) must immediately take any action within their authorised power to safeguard or resolve the situation (e.g. disconnect any infected machine from the network (remove the cable) and notify the ICT Helpdesk) and notify a senior manager.

Reporting misuse

If any employee suspects activity which may constitute misuse or activities which could jeopardise system security, they must report this immediately to a senior manager. The senior manager must consider whether it would be appropriate to involve Internal Audit and must always ensure that all relevant records and documents (paper and electronic) are safeguarded and retained securely. If necessary, a strategy for investigation will be agreed between the manager, Internal Audit and County Personnel, taking legal advice as necessary.

Legislation

Users should understand the relevant legislation relating to Information Security and Data Protection, and should be aware of their responsibilities under this legislation. The following statutory legislation governs aspects of the School's information security arrangements. This list is not exhaustive :

- The Copyright Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Electronic Communications Act 2000
- The Regulation of Investigatory Powers Act 2000
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The re-use of Public Sector Information Regulations 2005

Consequences of breach:

Disciplinary action

Breaches of this policy may result in the application of the Disciplinary Procedure and may, if deemed sufficiently serious, be treated as gross misconduct. In the case of Contractors, agency staff, volunteers or partnership employees, breach may result in termination of the contract or relevant arrangement and/or withdrawal of the relevant facility. Police involvement and prosecution may follow if the conduct in question constitutes possible criminal activity.

I confirm that I have read, understood and will adhere to Wistaston Academy's Acceptable Use Policy.

Signed: …….. Date: ……