Middlewich High School

ICT Acceptable Use Policy and Practice 2019

Date Agreed by staff and governors:
Next review date: January 2022

"Achievement for All"

CONTENTS:

PURPOSE

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

The School 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)
- tablets and smartphones
- telephones (hard wired and mobile)
- pagers
- fax equipment
- computers – *this covers ANY computer used for work purposes, whether at the place of work or elsewhere* (*see Laptops For Teachers*)
- 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 School (e.g. volunteers). It takes account of the requirements and expectations of all relevant legislation.

Headteachers 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 Headteacher 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.

Headteachers 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

Use of Facilities

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 the Headteacher or an appropriate line manager. This will usually be in writing or may be covered by the parameters agreed by the Headteacher with the team.

Facilities for Private Use

If an employee needs to use a School phone (e.g. at their desk) for private purposes that are permissible within this policy, the call should be timed and the office given the details immediately to enable the cost to be charged to the employee. Payment is not required where employees need to phone to notify someone they have been delayed at work or in other emergencies.

In terms of using other equipment and materials, the decision to allow such use is at the Headteacher'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. The Headteacher or 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 team.

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 school 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 School 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.

INADVERTENT ACCESS TO INAPPROPRIATE SITES AND INAPPROPRIATE EMAILS

If an employee inadvertently accesses an inappropriate web site, they should leave it immediately but notify the Headteacher/Senior 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 school's/Council's policy. If there is repetition, the employee should retain the messages and notify their Headteacher/Manager. If the emails are racist or sexist or could otherwise be regarded as offensive, they should be left in the inbox and the Headteacher/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.

SCHOOL 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, at intervals thereafter and possibly through automatic messages on school equipment, that, in relation to any electronic communication, there can be no expectation of absolute privacy when using school/County 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**. 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. It would only be authorised following the advice of the Council's Statutory Officers. Where calls are made via the CCC network, 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. Telephone response times will be sampled from time to time.
- **Emails**. When using the Cheshire East County Council network, every incoming and outgoing email message is automatically swept for key words which could indicate misuse. The school reserves the right to apply similar screening to its own email systems.
- **Web access**. When using the Cheshire East County Council network, 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. The school reserves the right to apply similar restrictions and screening to its own web access systems.
- **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 Headteacher, manager, secretary or colleague.

ACCESS TO AND RETENTION OF MONITORING INFORMATION

In the case of Cheshire East County Council systems, access to routine monitoring information is restricted to specified employees in Information & Communication Technology Services and Audit. If they identify a potential issue of abuse the relevant Headteacher/Senior Manager will be given access to the information to 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. This information would be held by the Headteacher, accessible by the Headteacher and if appropriate other Senior Staff, Governors.

SURVEILLANCE

Permanently fitted CCTV cameras are installed by the School, in the Reflection (internal isolation) room, on the corridor by room 5 and in the central library area, for security and safety reasons and will always be visible to people within their range. Video recording, onto the computer server, 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. CCTV cameras also cover areas around the sports hall and dining room, these are owned and managed by Congleton Borough Council.

Covert monitoring will only be used in connection with a criminal investigation or where abuse of terms of employment, e.g. the sickness scheme, is being investigated. This will always be in accordance with the statutory safeguards applicable to such activity (the Regulation of Investigatory Powers Act and the Human Rights Act) and only authorised following careful consideration of the need for such action in accordance with the attached policy entitled "Surveillance under the Regulation of Investigatory Powers Act 2000".

This policy provides safeguards in relation to who can sanction covert surveillance (only the Monitoring Officer (County Solicitor) or his authorised deputy), the reasons it can be undertaken and how long it can continue.

SECURITY

Every employee must observe the school's/Council's communications and information technology security requirements (as detailed in the ICT Code of Practice) and act responsibly when using equipment and materials. Employees will be provided with the necessary briefing and training to enable them to comply with this requirement. The Headteacher 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, if appropriate, notify the person responsible for ICT) and notify the Headteacher or 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 the Headteacher or a senior manager. The Headteacher or 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 Headteacher/manager, Internal Audit and Schools' HR Consultancy, taking legal advice as necessary.

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.

STAFF LAPTOP LOAN CONDITIONS

A laptop computer will be loaned to you while you remain employed by Middlewich High School. While the laptop is in your care the following items should be noted:

1 The Laptop remains the property of Middlewich High School. The laptop is for use in connection with MHS business only.

2 All laptops are issued to a **nominated** member of staff, it is this member of staff who is **responsible** for making sure that the laptop is **kept secure at all times**.

3 MHS Insurance cover provides protection from standard risks **but excludes** theft from an un-attended car.

4 Due to the increasing number of viruses that take advantage of operating system attacks Anti Virus and Windows Update must be carried out at a regularly. This is automatic when connected to the MHS network. It is the nominated member of staff's responsibility to make sure the laptop's security is up to date.

5 Should any faults occur the school's IT support staff must be advised as soon as possible so that they may undertake any necessary repairs. Under no circumstances should staff attempt to fix suspected hardware faults.

6 Any charges incurred by using this laptop outside business use are not chargeable to the school. These charges will be the responsibility of the nominated member of staff.

7 Upon temporary or permanent loss of the laptop, the police should be notified immediately. The IT network manager should be informed as soon as is practical with a report of the circumstances, police incident number and a list of all business data lost, specifically detailing **confidential data** secure or unsecure (normal logon password is classed as unsecure).

8 Software **licensed by the school**, authorised by the Headteacher, or Network Manager on his behalf, and installed by the school's IT support staff is the only software that the school takes legal responsibility for. Installed software will be checked during regular routine maintenance carried out by IT support staff and any irregularities reported to the network manager who may forward this information to the Headteacher or LA. Any software that is installed on the laptop that is not installed by IT Support is the legal responsibility of the nominated member of staff that the laptop belongs to, and not that of the school.

MIDDLEWICH HIGH SCHOOL

COMMUNICATIONS AND INFORMATION

ACCEPTABLE USE POLICY – including use of laptops

Name: _____

I have received and read a copy of the Middlewich High School Communications and Information Acceptable Use Policy and agree to abide by the procedures and guidance contained within it.

Signed _____

Date _____

Please complete the following information

Laptop Make _____

Model _____

Serial Number _____

Service Tag No. _____

Date Issued _____