



Eccleston C.E. Primary School
Let Our Light Shine

Acceptable Use Policy

Pupil Welfare, Community and Safeguarding Committee

Reviewed: Spring 2018

Approved by Pupil Welfare, Community and Safeguarding Committee:
Spring 2018

Approved by Full Governing Board: Spring 2018

Signed by Chair of Governors:

Review Date: Spring 2021

ECCLESTON C.E. PRIMARY SCHOOL

Acceptable Use Policy

PURPOSE

The policy has been developed to advise employees of 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 / Council 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 - *this covers ANY computer used for work purposes, whether at the place of work or elsewhere*
- 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.

The Headteacher will discuss the policy with staff and agree parameters within which they will act. 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 the Headteacher in the first instance.

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

The Headteacher 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

The school's/Council's Code of Conduct for Officers states 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 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.

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 Head teacher'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/Council 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/Council 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

SCHOOL/COUNCIL 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/Council equipment, that, in relation to any electronic communication, there can be no expectation of absolute privacy when using school/Council equipment provided for official/ work purposes; and that the school/Council 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/Council 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 Cheshire West and Chester 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 West and Chester 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 West and Chester 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 West and Chester 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.

SURVEILLANCE

Permanently fitted surveillance cameras are installed by the Council or 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.

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 and only authorised following careful consideration of the need for such action.

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 or use the Confidential Reporting Procedure (see Section A27). 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, 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.