Duddon Saint Peter's CE 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/Local Authority'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. The School/LA recognises employees' rights to privacy but needs to balance this with the requirement to act appropriately. 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 a 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, eg.

- mail systems (internal or 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, agency staff and 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 (eg. volunteers). It takes account of the requirements and expectations of all relevant legislation.

Every employee will have the policy explained to them on induction and be given a copy for future reference.

Use of equipment and materials

Use of facilities
The LA Code of Conduct 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.

Facilities for private use
To encourage employees to use and learn about ICT methods and means and to meet reasonable private needs, the School/LA have provided computing equipment for professional use during an employee's own time.

Members of staff may use the school phone for private purposes that are permissible within this policy. In terms of using other equipment and materials, the decision to allow such use is at the Head Teacher's discretion. 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
ICT Code of Practice

It is not acceptable to use school/LA 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 distasteful or offensive sites
using message encryption or anonymised web searches
employment diversity policies
actions which embarrass the school/LA or bring it into disrepute

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 the 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 ('clean jokes'), the recipient should point out to the sender that they do not wish to receive such material 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 material and keep a record of doing so.

School/LA monitoring

All employees should be made aware that in relation to any electronic communication, there can be no expectation of absolute privacy when using school/LA equipment and that the school reserves the right to monitor all communications including their content.

Emails are automatically swept for key words which could indicate misuse. Access to some web sites is automatically prevented and others are restricted. An automatic record of all sites visited is made to identify inappropriate sites. The privacy of internal and external mail marked 'personal' will normally be respected.

Access to and retention of monitoring information

Access to routine monitoring information is restricted to specified employees in ICT Services and Audit. Their reports can be made available to managers to enable any action to be taken.

Surveillance

Permanently fitted surveillance cameras are installed by the school for security and safety reasons and are visible to people within their range. Video recordings are kept secure and information used only for security purposes.

Security

Every employee must observe the school/LA's communications and information technology security requirements and act responsibly when using equipment and materials. Any employee detecting a potential security problem (eg. virus or unauthorised access) must immediately take any action to safeguard or resolve the situation and notify the Helpdesk.

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 manager or use the Confidential Reporting Procedure. The manager must consider whether it is appropriate to involve Internal Audit and must ensure that all relevant documents are safeguarded and retained securely.

Consequences of breach: disciplinary action
Breaches of this policy may result in the application of the Disciplinary Procedure and may be treated as gross misconduct. Police involvement and prosecution may follow if the conduct in question constitutes possible criminal activity.

Date*:* *March 2023* Date of review: *Spring 2025*