



Acceptable Use Policy For ICT

Pikemere School

The Acceptable Use Policy for ICT in respect of Pikemere School has been discussed and adopted by the Governing Board.

Chair of Governing Board: *Christine Richards* Mrs C Richards

Head Teacher: *S. L. Gohr.* Mrs S L Gohr

Agreed and ratified by the Governing Board on: 22nd January 2020

Policy Review Date: Spring 2023



Communications and Information Acceptable Use Policy

Acceptable use Policy for ICT

Information Technology (IT) is an increasingly integral part of Pikemere School's activities and is essential in the delivery of most services. Most school employees will use the school's Information Communication Technology (ICT) in the course of their duties.

This policy is designed to enable the School to:

- get the best return possible for the investment it has made in technology
- gain maximum benefit from email and the internet
- comply with the law
- minimise legal and other risks associated with the use of technology
- ensure effective running of the school's business
- minimise the risk of disruption caused by computer viruses and inappropriate use of IT; and
- provide clear information to employees and to increase ICT skills of our employees.

This document sets out the school's policy on using its computers and networks, including all devices such as telephones, mobile phones; printers, scanners and anything of an electronic nature otherwise referred to as information technology etc. This equipment is, for clarity of understanding, referred to throughout this policy as the Systems.

This policy applies to all school employees who use the Systems. It also applies to other people using the Systems such as agency workers, contractors' staff and volunteers.

It is based on the Government Connect Code of Connection and the ISO27001 / BS7799 standards for information management and security and is designed to provide a safe and secure environment for the use of technology.

Employees should be aware that the school Systems including the internal and external e-mail system may be monitored from time to time to ensure that the system is not being abused, to ensure that this policy is being complied with and for any other lawful purpose.

If you are unsure about how a rule or requirement applies then discuss with the Headteacher.

All users are required to read and accept this Acceptable Use Policy.



Email Policy

Emails form part of the school's corporate records and E-mails sent or received while on school business or using school facilities are the property of the school.

- Managers should ensure that staff use email in accordance with this Code.
- The sending and receipt of personal email messages is permitted as long as it does not interfere with work commitments. See section 8.
- Personal home email accounts should not be used to conduct school business with the public or external organisations.
- Users must not set up 'automatic' forwarding arrangements for any messages from their work account to one outside the authority, e.g. at home. Automatically sending authority emails to external accounts increases the risk of disclosure or interception.
- Each user is responsible for the context of all text, audio and images that they send. They should ensure that private emails cannot be misinterpreted as the views of the school and do not contradict our policies or interests.
- No email or other electronic communications may be sent which misrepresents the sender as anyone else.
- The email service should not be used for transmitting, accessing, retrieving or storing any communications of a discriminatory or harassing nature or that are racist, offensive, obscene, pornographic, or sexually explicit. This applies to both business and personal use.
- The sending or forwarding of chain letters or other unauthorised mass mailings, regardless of the subject matter, is not allowed.
- Treat suspect email or that from a dubious source with caution. Do not reply or forward (even to ICT) a message if there is any doubt. Similarly do not open attachments or click on web links on suspect emails, as this could activate computer viruses or other malicious processes.
- The sending of unwanted messages can constitute harassment. Careless use of language can lead to a bullying tone and can also be considered harassment.
- Do not send (or forward) email containing derogatory statements, potentially libellous, defamatory, comments likely to cause offence, gossip, hoaxes, or jokes to others inside or outside the school or Trust. See section 11
- Use 'shortcuts' or hyperlinks wherever possible, instead of attaching documents to emails. Large attachments (i.e. over 5Mb) should be avoided.



Use of the Internet

Users are granted access to the internet for business purposes and light personal use (see Section 8). Users must ensure that they comply with the provisions set out in this Code of Practice.

- The school maintains an awareness of staff Internet usage.
- Access to gambling, pornographic sites and sites of a similar nature, is not allowed under any circumstances.
- School or Trust information which is intended for internal use only, must not be placed on a system or website that is publicly accessible via the Internet.
- Staff should only enter personal information, e.g. credit card numbers, log in passwords etc. to websites if access to the site is encrypted, i.e. a 'padlock' symbol is shown in the bottom corner of the screen.
- The Internet is an insecure medium, therefore confidential or sensitive documents should only be sent by methods agreed to be secure. Guidance can be sought from the school office.
- It can be difficult to verify the true identity of a third party on the Internet. For your own safety and security and to protect the school, information should not be shared with other users unless their identity is certain.
- Care must be taken using Social Networking sites in and out of work. The same care must be taken when posting information as sending email or writing official letters (see [Social Networking advice in the staff handbook](#))
- The School does not accept liability for any loss or damage arising from use of the Internet to make personal financial transactions.

Password and Security

Passwords protect information against accidental or malicious disclosure, modification or destruction. Information is an important and valuable asset which must be managed with care.

Users should follow good password practices:

- A password should be at least seven characters in length.
- Contain characters from three of the four categories: uppercase; lowercase; 0 through 9; or special characters
- Not contain two of the same characters consecutively.
- Be difficult for anyone else to guess.
- Be kept confidential and not shared with anyone, not written down, and not included as part of an automated routine e.g. stored in a macro.
- Be changed regularly and not used again for at least 12 months



Users must 'log out' of systems fully or use the 'lock computer' command when leaving a workstation unattended.

The school office ensures that staff have appropriate system access rights to undertake their roles, and that when an employee leaves or moves from their department that their system access rights are revoked.

Mobile Working

Mobile working, whether at home or away from normal business locations, brings with it additional threats to data security. Mobile equipment is also more vulnerable to theft, loss or unauthorised access.

While the other provisions of this policy apply equally when working on school data or equipment while outside school premises, additional requirements apply to mobile phones, laptop and desk-top PCs.

- The school office maintains records for the booking out of equipment.
- Always ensure that equipment and media are powered off when left unattended and preferably locked away.
- Equipment must be carried as hand luggage when travelling. If carried by vehicle, the equipment must be locked out of sight. It should not be left in an unattended vehicle, even if locked out of sight, for any length of time e.g. overnight.
- Ensure that only equipment belonging to the school is connected to the school network.

Software and Virus protection

The School adheres strictly to software licence agreements.

- Staff should not load any software onto the school systems or school laptops.
- Users should not copy software nor use unlicensed copies of software.
- Care should be taken to prevent and detect the introduction of viruses and other malicious software by adhering to this policy.

However, if you suspect a virus on any School equipment:

- Inform the school office so that the school's ICT contractor can be informed.
- Unplug the network cable to isolate the PC
- Prevent anyone from using the PC.



Readable Information

Information from ICT systems is made readable on printed reports and computer display screens

- The school ensures that where the public have access to the school buildings that computer screens are located out of the view of the public, in order to protect confidential or sensitive information.
- Users should make sure that when using a mobile phone or laptop away from the office, including use at home, that unauthorised individuals are not able to view or overhear confidential or sensitive information.
- Sensitive or critical business information should be locked away (ideally in a fire- resistant safe or cabinet) when not required, especially outside working hours.
- Prints of sensitive information should be cleared from printers immediately.
- Where a printer is not within the view of the user, it is recommended that, where possible, “locked” or secure printing is used, i.e. it is necessary to enter a code or user name into the printer before the document is printed.

Personal Use

The school recognises that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the school permits you to use the Systems for personal use.

However, you must not allow personal use of Systems to interfere with your day to day duties. Excessive non-job related use of the Systems may be subject to disciplinary action.

Please be reminded that the internet and email service should not be used for transmitting, accessing, retrieving or storing any communications of a discriminatory or harassing nature or that are racist, offensive, obscene, pornographic, or sexually explicit. This applies to both business and personal use and is not allowed under any circumstances. Failure to adhere to this will result in disciplinary action (see section 12).

As mentioned above, all school Systems, including the external e- mail system and internet usage may be monitored from time to time to ensure that the system is not being abused, to ensure that this policy is being complied with and for any other lawful purpose.

You are responsible for any non business related file which is stored on your computer.



Ownership Rights

You should note that all information and files created, received, stored or sent by you while on school business or using school facilities form part of the school's corporate records and remain property of the school.

Health and Safety – Display Screen Equipment Regulations

All employees have responsibility for Health & Safety in the workplace, and this will be reflected in the manner that IT is used. Employees and Managers are expected to ensure that the use of technology in their areas complies with the provisions of Health and Safety legislation and that the presence of technology in the office is not a cause for concern.

There are specific requirements for Display Screen Equipment (DSE) users and, so far as the school is concerned, an employee falls within the requirements of the DSE regulations if they use equipment for continuous spells of an hour or more (on average) every day. All such employees are required to complete a DSE risk self- assessment. These risk assessment forms, along with additional advice and guidance, can be found at:

<http://www.hse.gov.uk/msd/dse>

Harassment and Abuse

The use of technology to harass and abuse others will not be tolerated. The school has a clear and fundamental commitment to equal opportunities and the welfare of its employees and will not tolerate harassment in any form. This commitment is made explicit in the current 'Dignity at Work Policy' which can be obtained from the school office.

Any employee found to be using technology as a means of harassing others will be investigated and disciplinary action will be taken as appropriate. This applies whether it is another employee or a member of the public who is subject to the harassment or abuse.

If an employee experiences harassment in any way they are urged to contact the Headteacher or Chair of Governors for advice and assistance.

Disciplinary Implications

Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the Computer Misuse Act 1990, and may lead to prosecution of the school and the individual(s) concerned and/or civil claims for damages.