



**Park View School**  
Together We Grow Stronger

# Park View School

## Acceptable Use Policy IT

Reviewed on: 06/10/2021  
Next review date: October 2023  
Authorised by Chair of Governors

Signature: *N. Fraser* .....

Name: Noreen Fraser

## **Contents:**

1. [Overview](#)
2. [Policy](#)
3. [Procedure](#)
4. [Authorised Use of the IT Facilities](#)
5. [Authorised Use of the Communications Facilities](#)
6. [Unauthorised Use of the IT Facilities](#)
7. [Unauthorised Use of the Communications Facilities](#)
8. [Staff Mobile Phones](#)
9. [Implementation of the Policy](#)
10. [General IT Information](#)
11. [ICT Technician's Duties](#)

## 1. Overview

The IT Facilities at Park View School are defined as:

- Computers and the software
- Monitors
- Keyboards
- Mouses
- Printers
- Scanners
- Cameras
- Camcorders
- Other devices including furnishings and fittings used with them

The Communication facilities at Park View School are defined as:

- Telephones
- Fax Machines
- Televisions
- Video Players
- DVD players
- Satellite Receivers
- Other devices including fittings used with them

Internet and E-mail can be defined as a Communication facility used in conjunction with IT facilities, as such; these will coincide with the IT Facilities.

This policy contains:

- Park View school's view on the use of e-mail and the internet at work.
- An explanation on what you can or cannot do.
- The consequences if you fail to follow the rules set out in this policy.
- General information relating to ICT, including the Data Protection Act.
- How the policy is implemented.
- The ICT Technicians duties to the ICT policy.

## 2. Policy

The use of the IT facilities within the school is encouraged, as its appropriate use facilitates communication and can improve efficiency.

Used correctly, it is a tool that is of assistance to employees. Its inappropriate use, however, causes many problems, ranging from minor distractions to exposing the school to financial, technical, commercial and legal risks.

Staff should always be an example of good practice to the students, serving as a positive role model in every aspect. Abuse of the ICT Facilities could result in the facilities being removed. Staff should always be aware of ICT use, misuse of the facilities, as defined in this policy, must be reported to the Head Teacher.

Since ICT facilities are also used by students, there should be a policy outlining their use of facilities. Staff should make sure that pupils comply with the policy.

Students misusing the ICT facilities must be reported to the Head Teacher. This policy applies to any personal computer connected to Park View School network and computers.

Any breach of the rules in this policy may result in disciplinary action being taken against you, which may lead to dismissal. A misuse or breach of this policy could also result in criminal or civil actions being brought against you or the school.

### **3. Procedure**

#### **E-mail and the Internet**

The schools' e-mail system and Internet connection are available for communication and use on matters directly concerned with school business. Employees using the schools e-mail system and Internet connection should give particular attention to the following points.

- **Appropriateness of e-mail**

E-mail should not be used, unless not possible, as a substitute for face-to-face communication. "Flame-mails" (e-mails that are abusive) can be a source of stress and can damage work relationships. Hasty messages, sent without proper consideration, can cause unnecessary misunderstanding.

- **The visibility of e-mail**

If the message is confidential, the user must ensure that the necessary steps are taken to protect confidentiality. The School will be liable for any defamatory information circulated either within the School or to external contacts.

- **Un-Solicited E-mail (SPAM)**

Park View School E-mail system and accounts must never be registered or subscribed to SPAM. Never disclose any of Park View School E-mail addresses without confirming that they will not be subjected to SPAM or if they will not be sold on to marketing companies.

- All e-mails that are sent or received must be retained within the School for a period of six months.
- All e-mails being sent to external recipients must contain Park View School standard confidentiality notice. That notice is normally configured as a signature by the ICT Technician and must not be removed.
- Non-text e-mails (containing graphics or colour) and e-mail attachments may contain harmful materials and computer viruses, which can seriously affect Park View School's IT Facilities. If unsure, seek assistance or approval from the ICT Technician.
- Offers or contracts sent via e-mail or the Internet are as legally binding on the School as those sent on paper. An exchange of e-mails can lead to a contract being formed between you, or the school, and the recipient. Never commit the school to any obligations by e-mail or the Internet without ensuring that you have the authority to do so. If you have any concerns, contact the Head Teacher.

- Buying online is only permitted with the Deputy Head or Head Teacher present, due to complying with monitoring and accountability. Hard copies of the purchase must be made, for yourself and for the finance manager. This is in addition to any purchasing arrangement followed according to school policy.

Any failure to follow this policy satisfactorily may result in disciplinary action, including summary dismissal.

#### **4. Authorised Use of the IT Facilities**

The IT facilities should only be used as required by your work duties. This includes, but may not be limited to:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching for any school related task
- Any School encouraged tuition or educational use
- Collating or processing information for school business
- Personal e-mail accounts are only permitted to be used if they have built-in anti-virus protection approved by the ICT Technician. Access to your personal e-mail must never interfere with your work duties.

#### **5. Authorised Use of the Communications Facilities**

The communication facilities should only be used as required by your work duties.

This includes, but may not be limited to:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching for any school related task.
- Any school encouraged tuition or educational use.

If unsure about your required use, please seek authorisation from the Head Teacher.

#### **6. Unauthorised Use of the IT Facilities**

You are NOT permitted under any circumstance to:

1. Use the IT facilities for commercial or financial gain without the explicit written authorisation from the Head Teacher.
2. Physically damage the IT facilities.
3. Re-locate, take off-site or otherwise interfere with the IT facilities without the authorisation of the ICT Technician or Head Teacher.

Certain items are asset registered and security marked, their location is recorded by the Site Manager for accountability, once items are moved after authorisation, you have a responsibility to notify the financial assistant of the new location. The exception to this point, is when items are moved to the designated secure room for insurance purposes over holiday periods.

4. Use or attempt to use someone else's user account. All users of the IT Facilities will be issued with a unique user account and password. The password must be changed at regular intervals. User account passwords must never be disclosed to or by anyone. This comes under the Computer Misuse Act and is illegal.
5. Use the IT facilities at any time to access, download, send, receive, view or display any of the following:
  - Any material that is illegal
  - Any message that could constitute bullying, harassment (including on the grounds of sex, race religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
  - Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
  - Online gambling
  - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
  - Any sexually explicit content

If you are subjected to or know about harassment or bullying, you are encouraged to report this immediately to your line senior or the Head Teacher.

6. Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
7. Install hardware or software without the consent of the ICT Technician or the Head Teacher.
8. Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the IT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of Park View School computers.

This comes under the Computer Misuse Act and is illegal.

9. Use or attempt to use Park View School IT facilities to undertake any form of piracy including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
10. Purchase any IT facilities without the consent of the ICT technician or Head Teacher. This is in addition to any purchasing arrangements followed according to School Policy.
11. Use or attempt to use the schools' phone lines for Internet or email access unless given authorisation by the Head Teacher. This includes using or attempting to use any other form of hardware capable of telecommunication regardless of ownership.
12. Use any chat-lines, bulletin boards or pay to view sites on the Internet. In addition, you must not download or attempt to download any software.

13. Use the Internet for any auctioning activity or to purchase items unless given authority to do so by the Head Teacher. This is in addition to any purchasing arrangement followed according to school policy.
14. Knowingly distribute or introduce a virus or harmful code onto Park View School network or Computers. Doing so may be subject to disciplinary action including to summary dismissal.
15. Use the IT facilities for personal use without the authorisation of the Head Teacher. This authorisation must be requested on each occasion of personal use.
16. Copy, download or distribute any material from the Internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
17. To obtain and post on the internet or send via email any confidential information about other employees, the School, its customers or suppliers.

Any unauthorised use of email of the Internet is likely to result in disciplinary action including summary dismissal.

18. Interfere with someone else's use of the IT facilities.
19. Be wasteful of IT resources, particularly printer ink, toner and paper.
20. Use the IT facilities when it will interfere with your responsibilities to supervise students.

## **7. Unauthorised Use of the Communications Facilities**

You are not permitted under any circumstance to:

1. Use the communication facilities for commercial or financial gain without the explicit written authorisation from the Head Teacher.
2. Physically damage the communication facilities.
3. Use of the communication facilities for personal use is not permitted without authorisation of the Head Teacher with the exception of the following point.
4. Use of Park View School telephone facilities for personal use is permitted for necessary calls lasting less than 10 minutes. Should you need to use the telephones for longer than this, then authorisation must be sought from the Head Teacher. This authorisation must be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls, you should however, notify the Duty Head or Head Teacher after the call. Any personal use of the telephones may be subject to a charge; this is at the Head Teachers discretion.
5. Re-locate, take off-site or otherwise interfere with the communication facilities without the authorisation of the Duty Head or Head Teacher.

Certain items are asset registered and security marked, their location is recorded by the financial assistant for accountability, once items are moved after authorisation, and you have a responsibility to notify the financial assistant of their new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.

6. Use the communication facilities at any time to access, receive, view or display any of the following:
  - Any material that is illegal.
  - Any material that could constitute bullying, harassment (including on the grounds of sex, race religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations.
  - Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age.
  - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false.
  - Any sexually explicit material.
  - Any adult or chat-line phone numbers.

If you are subjected to or know about harassment or bullying, you are encouraged to report to your line senior or Head Teacher

7. Use or attempt to use Park View School Communication facilities to undertake ANY form of piracy including the infringement of media rights or other copyright provisions whether knowingly or not. This is illegal.
8. Use or attempt to use the school's communication facilities for internet or email access unless given authorisation by the Head Teacher. This includes using or attempting to use any other form of hardware capable of telecommunication regardless of ownership.
9. Copy, record or distribute any material from or with the communication facilities that may be illegal to do so. This can include television media, films, telephone conversations and music. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
10. Use or attempt to use the communication facilities to call overseas without the authorisation of the Head Teacher.
11. Use the Communication facilities when it will interfere with your responsibilities to supervise Students.



## 8. Staff Mobile Phones

### 1. Personal mobile phones

Staff should not use or carry their personal mobile phone whilst at work. If staff require their personal mobile phone during their working hours, this needs to be agreed by their Line Manager or a member of SLT.

Personal Mobile phones should be kept away in staff member's personal belongings i.e. bag/coat. Lockers are available in the staff room to keep any personal items.

### 2. Work issued mobile phones

Park View School will issue staff with a work mobile phone if they see necessary. The following is outlined in the **Staff Mobile Phone User Agreement**, and are the conditions under which the staff will accept the provision of a mobile phone from Park View School.

The school retains sole right of possession of the mobile phone and related equipment, and may transfer the mobile phone to another teacher if you do not, or are unable to, for any reason, fulfil the requirements of this agreement.

#### **Under this agreement the school will:**

1. Provide a mobile phone for your sole use while you are a permanent full-time or part-time member of staff at the school.
2. Set up the mobile phone to enable you to connect to and make effective use of the school network.
3. Plan and manage the integration of the mobile phone into the school environment, and provide the professional development required to enable you to use the mobile phone effectively.
4. When required, expect you to pay an excess for accidental damage or loss, or repair/replacement costs where loss or damage is a result of your own negligence.
5. Make regular payment to the leasing company for the mobile phone.
6. Receive an itemised bill on a monthly basis. Any personal usage will be charged directly to the member of staff concerned (as per internal audit requirements).

#### **Under this agreement, you will:**

1. Bring the mobile phone and charging unit to the school each day and keep the mobile phone with you or within your sight at all times.
2. Transport the mobile phone safely using the cover issued with the mobile phone.
3. Not permit any other individual to use the mobile phone without your supervision unless agreed by the Head Teacher.
4. Take responsibility for any other individual using the mobile phone.
5. Provide suitable care for the mobile phone at all times and not do anything that would permanently alter it in any way.
6. Not use the mobile phone in ways which could damage the reputation of the school or your own career.
7. Only download apps and content from reputable sources.
8. Lock the mobile phone screen when not in use with a passcode.

9. Keep the mobile phone clean.
10. Immediately report any damage or loss of the mobile phone to the Business Manager.
11. Immediately report any viruses or reduced functionality following a download to the Business Manager.
12. Be prepared to cover the insurance excess, repair or replace the mobile phone when the damage or loss has been a result of your own negligence.
13. Attend any training sessions offered by the school.
14. Make arrangements for the return of the mobile phone and passcode to the School Office if your employment ends or if you will be away from the school for an extended period.
15. Use the mobile phone in a way which does not contravene the policies and procedures of Park View School including the ICT Policy, Data Protection Policy and Safeguarding Policy.
16. Keep the phone well charged ready for use when in school.

Insurance cover provides protection from the standard risks while the mobile phone is on the school site or in your home **but excludes** theft from your car or from other establishments. Should you leave the mobile phone unattended and it is stolen, you will be responsible for its replacement and may need to claim this from your own insurance company or pay from your own pocket.

Failure to agree to or to abide by these terms will lead to the mobile phone being returned to the school and serious breaches may lead to disciplinary action.

## 9. Implementation of the Policy

1. Staff are requested to report any breach of this policy to the Head Teacher.
2. Regular monitoring and recording of e-mail messages will be carried out on a random basis. Hard copies of e-mail messages can be used as evidence in disciplinary proceedings.
3. Use of the telephone system is logged and monitored.
4. Use of Park View School internet connection is recorded and monitored.
5. The financial assistant randomly checks asset registered and security marked items.
6. The ICT technician checks computer logs on the school's network regularly. Unsuccessful and successful logons are logged on every computer connected to the school's network. Unsuccessful and successful software installations, security changes and items sent to the printer are also logged.
7. The ICT technician can remotely view or interact with any of the computers on the school network. This may be used randomly to implement the ICT policy and to assist in any difficulties.
8. The schools network has anti-virus software installed with a centralised administration package; any virus found is logged to this package.
9. Park View School database systems are computerised. Unless your line manager gives you express permission, you must not access the system. Failure to adhere to this

requirement may result in disciplinary action. All users of the database system will be issued with a unique individual password, which must be changed at regular intervals. Do not under any circumstances disclose this password to any other person.

Attempting to access the database using another employee's user account / password without prior authorisation is likely to result in disciplinary action, including summary dismissal.

10. User accounts are accessible by the Head Teacher and the ICT Technician.
11. Users must ensure that critical information is not stored solely within Park View School computer system. Hard copies must be kept or stored separately on the system. If necessary, documents must be password protected.
12. Users are required to be familiar with the requirements of the Data Protection Act 1998 and to ensure that they operate in accordance with the requirements of the Act. The obligations under the Act are complex but employees must adhere to the following rules
  - Do not disclose any information about a person including a pupil, without their permission which you would object to being disclosed about yourself
  - Such material includes information about a person's racial or ethnic origin, sex life, political beliefs, physical or mental health, trade union membership, religious beliefs, financial matters and criminal offences
  - Do not send any personal data outside the UK

## **10. General IT Information**

- Messages should be deleted on a regular basis after 6 months or stored in a suitable hard copy file.
- Information and data on the schools network and computers should be kept in an organised manor and should be placed in a location of an appropriate security level. If unsure, please seek help and information from the ICT Technician.
- Employees who feel that they have cause for complaint as a result of e-mail communications should raise the matter initially with their Line Manager, or Head Teacher as appropriate. The complaint can then be raised through the grievance procedure.

## **11. ICT Technician's Duties**

To monitor and affect accountability of the ICT policy, the ICT technician is requested by the Head Teacher to:

- Carry out daily checks of Internet activity of all user accounts and to report any inappropriate use to the line manager or Head Teacher.

- Monitor the computer logs on the school's network and to report any logged inappropriate use to the line manager or Head Teacher.
- The ICT Technician can remotely view or interact with any of the computers on the school network. This may be used randomly to implement the ICT policy and to assist in any difficulties.
- Access files and data to solve problems for a user with their authorisation, if an investigation is requested by the Head Teacher, authorisation from the user is not required.
- Adjust access rights and security privileges in the interest of the protection of school data, information, the school network and computers
- Disable user accounts of staff that do not follow the policy at the request of the Head Teacher
- Assist the Head Teacher in all matters requiring reconfiguration of security and access rights and in all matters relating to the IT policy.
- Assist staff with authorised use of the IT facilities if required.