Parkstone Grammar School

INTERNET AND E-MAIL ACCEPTABLE USE POLICY
Staff

DATE APPROVED	04/07/2017
APPROVED BY	Curriculum & Student Matters Committee
NEXT REVIEW	2019
TYPE OF POLICY	Non-Statutory

STAFF INTERNET AND E-MAIL ACCEPTABLE USE POLICY

Staff should read this policy carefully as they will, in the future, be deemed to be aware of its contents in the event that there is any breach of the School's policy.

PURPOSE

The purpose of this policy is to ensure that employees of Parkstone Grammar School understand the way in which Electronic mail (e-mail) and the Internet should be used in and out of School.

AIMS OF THE POLICY

This policy aims to ensure that e-mail and the Internet are used efficiently for their intended purpose without infringing legal requirements or creating unnecessary business risk.

SCOPE

All employees of Parkstone Grammar School including temporary staff are subject to this policy. Failure to comply with the policy may lead to disciplinary action, including dismissal. At the same time, their conduct and/or action(s) may be in contravention of the law and they may be personally liable.

GENERAL

All Parkstone Grammar School resources, including computers, e-mail and voicemail are provided primarily for the educational and business purposes of the school and for carrying out activities consistent with those purposes.

Incidental and occasional personal use of these systems is permitted, subject to the restrictions contained in this policy and with the approval of the Headteacher. Any personal use of the Internet or e-mail is expected to be in the employee's own time and must not interfere with the person's job responsibilities.

Staff must be aware at all times of the particular sensitivities applying in the school environment and of their responsibility to set a high moral example to students. Staff must not engage in any activity which is illegal, likely to cause offence or to have negative repercussions for the School. Staff must not upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

- are or might be considered to be indecent or obscene;
- are or might be offensive or abusive in that its content is or can be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful;
- encourage or promote activities which make unproductive use of their time;
- encourage or promote activities which would, if conducted, be illegal or unlawful;
- involve activities outside the scope of their responsibilities – for example, unauthorised selling/advertising of goods and services;
- might affect or have the potential to affect the performance of, damage or overload the School's system, network and/or external communications in any way, i.e. Spotify, Apple Music or other streaming services;
- might be defamatory or incur liability on the part of the School or adversely impact on the image of the School;
- Staff should be aware of any potential copyright infringement.

USE OF E-MAIL

Care should be taken when using e-mail. E-mail messages are perceived to be less formal than paper-based communication and there is a tendency to be lax about their content. Staff should bear in mind that they and the School will be held accountable for all expressions of fact, intention and opinion they communicate via e-mail can be held against them and/or the School in the same way as verbal and written expressions or statements.

Staff should not include anything in an e-mail which they cannot or are not prepared to account for. Staff should not make any statements on their own behalf or on behalf of the School, which may be considered defamatory or in any way damaging to the reputation of any person or entity.

E-mail messages which have been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending e-mail can be identified. E-mails, both in hard copy and electronic form, are admissible in a court of law.

Care must be taken in the distribution of e-mails to ensure that e-mails should only be sent to those who need to be aware of the content. “Blanket e-mails” eg “All at Parkstone Grammar School” should be used sparingly and NOT for sending e-mails that are not relevant to the School.

INTERNET E-MAIL

Access to certain e-mail internet sites is restricted due to the potential threat of viruses being spread and infecting the network. Please follow your security awareness testing and training guidelines and follow best practice.

SAFEGUARDING

This policy states restrictions of use for email and the internet to protect students.

CORE SCHOOL VALUES

The school aims to provide a balanced curriculum which will enable all girls to develop to the full the skills and attitudes with which to cope with adult life in a rapidly changing and increasingly technological and scientific society. This policy recognises the benefits to learning from offering students the opportunity to use personal ICT devices in school to support their development and learning.

STAFF & USE OF THE INTERNET

Staff should bear in mind at all times that when visiting an internet site their identity (which is linked to the School) may be logged. Therefore, any activity engaged in, undertaking given or transaction made may impact on the School.

Staff must:

- always ensure that the School is neither embarrassed nor liable in any way by their use of the internet. If in doubt, they should avoid such action.
- virus check all material which is down loaded from the internet or received from any external source. The same applies to any materials which they intend to load onto the system using their hard drive or from their CD drive or USB drive or cloud storage.
- not make any statements on their own behalf or on behalf of the School which may be defamatory of or in any way damaging to the reputation of any person or entity.

The following activities are expressly prohibited:

- the introduction of packet-sniffing or password detecting software.
- seeking to gain access to restricted areas of the network.
- the introduction of any form of computer virus.
- other hacking activities.
- knowingly seeking to access data which is known or ought to known to be confidential.
- knowingly accessing or downloading any material which is pornographic, offensive or illegal.

In addition to breaching the terms of their employment contract the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material (i.e. hacking).
- unauthorised access with intent to commit or facilitate the commission of further offences.
- unauthorised modification of computer material.

USE OF PHOTOS AND PERSONAL DETAILS

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet for ever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg. on social networking sites.

Staff are allowed to take digital/video images to support educational aims, but must follow school policy concerning the sharing, distribution and publication of those images.

USE OF VIDEO CONFERENCING / WEBCAMS / PHONE CAMERAS / TABLET CAMERAS

Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Photographs published on the school web site, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images.

Students' full names must not be used anywhere on a web site or blog, particularly in association with photographs / video

Written permission from parents or carers must be obtained before photographs / video of students are published on the school website.

CONFIDENTIALITY

All information relating to students or staff and the operation of the school is confidential. Staff are expected to treat electronic information with the same care as they would paper-based information which is confidential. They must keep all such information secure, use it only for the purpose(s) intended and must not disclose the same to any unauthorised third party (which may sometimes include other employees of the School).

- Staff must keep passwords safe, not disclose them to anyone and change in line with 90 day requirements
- If a document is highly confidential or sensitive in nature, it must be stored in a private directory or an equivalent password protected directory, or encrypted folder/laptop or IT supplied encrypted USB.
- Copies of confidential information should only be printed out as necessary (and retrieved from the printer immediately) and stored or destroyed in an appropriate manner

MONITORING

All Parkstone Grammar School resources, including computers, e-mail and voicemail are provided solely for school purposes.

At any time and without prior notice, Parkstone Grammar School maintains the right to examine any systems and inspect and review any and all data recorded in those systems. Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by the school. This monitoring helps to ensure compliance with internal policies, supports the performance of internal investigations, and assists the management of information systems.

Staff should be aware that it is highly likely that e-mail and internet traffic will be monitored and tracked.

If staff are unclear about any of the issues discussed in this Internet and E-mail policy, they should contact their Line Manager.

LINKED POLICIES

- Internet and Email Acceptable Use Policy – Students
- Internet Safety Policy
- Bring Your Own Device Policy