goffs School

Internet Usage Policy

Committee:	**Pastoral**
Author:	**Ben Pearce**
Date of issue:	**March 2014**
Amended:	**February 2015**
Reviewed Date:	**February 2016** (no change)
Review Date:	**February 2017**

GOFFS SCHOOL INTERNET USAGE POLICY – ALL STAFF, GOVERNORS AND VISITORS

This policy applies to all computer users, which means anyone who is authorised to use and/or access our computers, computer software, information and data whether such authorised use or access takes place during or outside of normal working hours and whether such authorised use or access takes place inside our premises or elsewhere, including by remote usage.

1) Access

All computer users are permitted access only to those parts of the computer system which they need to enter in order to carry out their normal duties. Any other access will be regarded as unauthorised.

Should a computer user believe that they need to gain access to other parts of the computer system, they must first seek clearance from the System Manager.

2) Computer Viruses

A computer virus is a piece of computer software or program designed to replicate itself from computer to computer without participation of the computer user. Once loaded into a computer, it can cause loss of data and programs on that computer or network and in extreme circumstances a virus may even damage the computer itself. Sources of viruses include the Internet, E-mail, CD-ROMs and disk drives.

All PC software that is purchased, installed and supported by the ICT Support Team can be guaranteed to be free of viruses. However, software and diskettes introduced via a route other than the ICT Support Team will not necessarily be free of viruses. Similarly, the copying of software from another PC, apart from being illegal, is one of the prime methods of helping viruses to spread. Users should check with ICT Support before downloading or installing any new software.

What you should do:

Ensure that the virus checking package on your computer is up to date. The ICT Support Team will remind you to update your virus software via e-mail and the bulletin.

What you should not do:

Make copies of our software. Copying commercial software for use on more than one machine is illegal.

Accept copies of software from others. If you have a legitimate need for the software you are being offered, then arrange for the ICT Support Team to either purchase it for you, or to check it thoroughly BEFORE it is loaded onto our systems.

If you think you have a virus you must contact the ICT Support Team immediately.

E-mail/Social Networking

- All communications by e-mail (both external and internal) are to be treated as if they are permanent written communications. All emails sent from a school or college account should be regarded as public, especially as a 'data subject access' request could be made under the Data Protection Act. Emails should always be in professional language and appropriate to being an employee.

- It should also be noted that where a private email account is used for issues associated with work, it has in some cases been deemed as a work account and therefore also subject to the rules of professional language and conduct. In short, to be safe, do not send a private email that you would not be happy for your employer or a colleague to read.

Private use of E-Mail/ Social Networking

Whilst it is accepted that computer users may send and receive limited personal communications by e-mail and social networking, these should be minimal and the privilege not abused, just as in the case of personal telephone calls. All computer users must ensure that any private use does not impinge on the performance of their duties.

Unacceptable Use of E-Mail/ Social Networking

There are certain types of communication which could give rise to liability both for yourself and potentially for us, and could potentially constitute a basis for dismissal. For this reason computer users should not send internally or externally or (where preventable) receive any personal or business e-mail or exchange material through social networking which:

- contains pornographic, obscene, defamatory, discriminatory or insulting material, whether or not you are offended personally by it

- contains information that is confidential, or may have contractual or other legal implications for us, except as part of your duties

- may damage our reputation or that of any person or organisation with which we deal

- includes derogatory remarks about other people or organisation (even if only sent internally). This includes the naming of or publishing of images of specific individuals or institutions

- makes representations or expresses opinions purporting to be ours, except where authorised

- may constitute sexual, racial or other harassment as specified in points above

Computer users are expressly warned that e-mail messages can be recreated even after deletion and may be used in legal proceedings.

Staff should:

- never give students their personal mobile number

- never link with students on any social media site unless it is via an official school site

- never exchange personal texts or calls with students

- never arrange to meet with students outside school apart from for official school events

3) SOCIAL NETWORKING SPECIFIC GUIDANCE FOR STAFF

Protect your professional reputation

- Your professional reputation is part of your current and future career so managing your online reputation is essential. **Anything that you post online is potentially public and permanent even if you have used privacy settings on your account.** On social media friends can re-post or comment on your posts which means others to whom you have not given access may view your comments.
- Think carefully before posting information online about our school, staff, students or parents – even if your account is private. Comments could be taken out of context and could be very damaging. The language you use is important, as abrupt or inappropriate posts may lead to complaints.
- Think carefully as to how you present yourself when you post images or when joining a group or 'liking' pages. These choices say something about you. An employer may reasonably believe that a recognisable member of staff putting an inappropriate post or image in the public domain will lower the reputation of the school and that could be a basis for disciplinary action. It is an implicit condition of employment that an employee owes a duty of loyalty to an employer. In addition, potential employers may also look online and you will want to consider whether your choices show you in the best light when applying for any future job.

Choose your friends carefully

- Think carefully about whom you are friends with online and which friends can access what information

- It is strongly advised that you do not accept friend requests, or requests to follow you, on your personal accounts from past students, (staff must absolutely not be "friends" with current students) or from parents of the school . By accepting such requests you could be making yourself vulnerable by sharing personal information, or by having access to personal information about students. This could leave you open to allegations of inappropriate contact or conduct and in addition, you could find yourself exposed to unwanted contact

Privacy settings

- When using social networking websites it is important that you are in control of who can see your account details and content including photos and albums, posts, status updates and any personal information. On Twitter, you can set your account to private by following these steps:

  Click on the 'settings and help' cog icon, found on the top right of the Twitter homepage > select 'settings' > select 'security and privacy' > tick the 'protect my tweets' check box > click 'save changes'

  By selecting the 'protect my tweets' option you will be able to either accept or decline requests to follow you

- For Facebook, choosing the 'Friends only' setting for every option enables you to achieve a good degree of privacy. Amend your Facebook privacy settings by following these steps:

  Click on the 'privacy settings' padlock icon, found on the top right of your wall > select either 'who can see my stuff' or 'who can contact me' > select 'friends' on the drop-down menu

  Updates to your privacy settings are automatically stored and do not need to be saved manually. Furthermore, you can customise each option and limit the information that certain people can see. It is always useful to use the 'view as' option, to check how your profile appears to others, and that the information you want to remain private or for 'friends only' is not visible to everyone. If you are not entirely sure about how to use all the settings, treat all of the information that you post as being available to everyone and act accordingly
- It is a good idea to remove any friends, or customise the privacy settings for current friends, if access to your personal activity could compromise your position. It is important, regardless of which setting you use, that you assume that every post you make could be made public, because 'friends' settings do not guarantee privacy
- Be careful about comments you post on your friends' walls; if their profile is not set to private, your posts will be visible to everyone. Sharing content with others could mean that you lose control of it; for example, friends could pass on your information
- Always use a strong password that contains a combination of upper and lowercase letters, and numbers and ensure that it is at least six characters long. Get in the habit of

logging out after you have finished online. Not logging out means the next user can access your social networking account. Do not select the 'remember the password' option when logging on to a shared computer or device as others may later be able to access it. On your mobile phone always set a PIN or passcode, so if you lose or mislay it, access to your account is still protected.

Ensuring that you have robust security settings on your social networking accounts could prevent them from being hacked. If an employee has kept up a reasonable degree of security and if the hacker clearly had to get through serious barriers, then the exposure of material could be excusable; there was a reasonable expectation of privacy.

Manage what others post about you online

- Search your name regularly online to monitor any content about yourself. This enables you to see what others can and provides an opportunity for you to delete anything that may compromise your reputation
- Other people could post images on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a friend online you should contact them and ask that the content be removed. Alternatively, you could go directly to Facebook to request that it be removed, although it will be Facebook's judgement as to whether they should be taken down or not
- In 2014 there was a European ruling against Google that the search giant must delete "inadequate, irrelevant or no longer relevant data" from its search results when requested. In theory this means that Google will need to remove links to personal information that is not relevant or in the public interest. However the reality is that requests will still have to go through the courts and could take a complicated battle to do so. The fact remains that the information will still be available on the web, it just won't be visible through a Google search

4) Internet Access

As in the case of e-mail, the school recognises that certain employees will have a legitimate need to access the Internet and also that a reasonable amount of access for personal purposes is acceptable.

Internet use to support activity connected with our ongoing operation, including client communication, research, administration and the development of professional knowledge is non-restricted.

Internet use for personal banking, ordering goods, searching for information outside of the scope of work is allowed provided it is reasonable and does not infringe on the performance of your duties.

Use of the school internet facilities to access, view, download, print or distribute pornographic, indecent, sexually explicit or obscene material or material likely to cause offence, whether or not this would constitute a criminal offence and irrespective of whether

you do so during working hours or whether you personally find such material insulting or distasteful is also prohibited, and could potentially constitute a basis for dismissal.

You may inadvertently access inappropriate material because of misleading site descriptions or innocent searches. If this should happen you should exit the site immediately and inform the Network Manager. Failure to do so with due speed may result in management concluding that you deliberately viewed the material.

5) Guidance on handling personal data in the computer system

We all need to be mindful of our legal obligations when creating, storing or circulating information about individuals. Information relating to any identifiable individual which is created on our computer systems (e.g. a word document or e-mail) counts as "personal data" for the purposes of the Data Protection Act 1998.

Once we hold personal data about an individual we have obligations relating to that data. We must ensure that the data is accurate, not excessive or irrelevant and we can "process" the data only if strict conditions are satisfied. In brief, most data can be processed for legitimate business reasons but sensitive information {e.g. about an individual's health) cannot usually be processed without specific consent. Circulating, retaining and even deleting information counts as processing.

Individuals have a right to see personal data that is held about them on our computer system. We may also have to disclose documents, including e-mails in the context of legal proceedings (whether or not they count as personal data.).

Against that background here is some practical guidance on handling information about individuals held on computer:

Beware what you say in e-mail messages or text messages If sending an e-mail about an individual, remember that this is likely to be processing personal data. This means that the individual may seek access to it and we have data protection obligations in respect of it. Consider whether a telephone call would be a more appropriate means of communicating the information.

Never ask for or send information about someone's health or other sensitive details unless they have specifically agreed to this or you know that you are acting within the limits of the Data Protection Act.

Remember that describing an individual by their initials ("ABC") or indirectly ("you know who..') will often still count as processing data about the individual.

Be careful about creating documents containing opinions about an individual. Personal data includes opinions about individuals, not just facts.

Never make "throw-away" remarks about individuals in e-mails, assuming that they won't see them. Subject access requests are becoming more common and this sort

of remark can lead to legal liability. Remember that e-mails are not a secure method of communication and can be forwarded very easily to individuals other than the intended recipients both deliberately and by mistake.

6) Monitoring of Internet and E-mail Use

All internet usage is logged automatically by the school systems, for security purposes. The source and destination of connection, time and number of bytes transferred are all logged.

A list of a email coming in and going out (including sender, recipient, time and subject) can be viewed by the Systems Manager at all times.

The school will monitor e-mails and internet usage:

- where the title of e-mail arriving on our server or the content of an attachment to an email alerts the Systems Manager to a breach of this policy or other inappropriate behaviour and they notify an appropriate senior manager accordingly

- where a breach of this policy, a breach of another policy, or other inappropriate behaviour is suspected

- to check for viruses

- if a member of staff is absent and e-mails need to be checked for work-related reasons

- Where the Principal has concerns regarding potential inappropriate use of email, and/or email not being used in line with school policy

The School has a duty of care to students and as such monitoring of e-mails and social networks is necessary. In most cases the Systems Manager will specifically warn you before introducing continuous monitoring of your internet usage or e-mails. However, in limited circumstances (for example - where warning you in this way would prejudice an investigation) the school may monitor without giving specific warning of this first. Social Networks may be monitored through use of keyword searches or by looking at publicly displayed content. All public content is subject to monitoring by both the school and external bodies.

Monitoring and checking of internet usage and e-mail will be conducted only by the Systems Manager or an appropriate senior manager. All computer users should note that marking e-mails as 'personal' does not mean that we will not in some circumstances see their content or attachments. If you do not wish the Systems Manager to read private e-mails you should make alternative arrangements that do not involve our property (for example, text messaging or web based email).

The Systems Manager may override any passwords or require computer users to disclose any passwords in order to facilitate access to any e-mail message for a reason set out above.

7) Consequences of breach of this policy

Failure to comply with any aspect of this policy without good reason could result in the removal of privileges to use the computer system for personal purposes and/or, in the case of employees, in disciplinary action being taken, and in the case of non-employees, termination of the relationship and/or legal action.

The following will be regarded as gross misconduct;

- serious breach of the school virus policy
- sending an e-mail which may materially damage the school's reputation or that of one of any person or organisation with which we deal
- sending an email which constitutes sexual, racial or other harassment
- deliberately using school internet facilities to access, view, download, print or distribute pornographic, indecent, sexually explicit or obscene material or material likely to cause offence

Computer users are specifically warned that there are a number of criminal offences that may arise from the misuse of our computer systems and that the school reserves the right to inform the police if we believe that such an offence may have been committed.

Please also see the Staff Acceptable Use Agreement.