ICT Acceptable Use (Staff)

Ellesmere Port Catholic High School

Approved by:	**Mr J Coucill, Chair of Governors**
Lead of Review:	**Mr C Jones, Business Manager**
Last reviewed on:	**November 2020**
Next review due by:	**October 2021**

Purpose

The policy has been developed to advise employees of when and under what conditions they may use Ellesmere Port Catholic High School's email 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 recognises employees' rights to privacy but needs to balance this with the requirement on the school to act appropriately, with probity, to safeguard its systems, and to be seen to be doing so.

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 work/life balance.

Scope

The policy applies to all employees and other individuals providing services/support to the school (e.g. volunteers & guests). It takes account of the requirements and expectations of all relevant legislation.

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, for example

- Internet and intranet (email, web access and video conferencing)
- EPCHS provided mail systems (internal and external)
- Web based personal email accounts e.g. Hotmail, virgin, yahoo, etc.
- Telephones (hard wired and mobile)
- Fax equipment
- Computers/ Laptops
- Photocopying, printing and reproduction equipment
- Recording / playback equipment
- Documents and publications (any type or format)

If at any stage employees require further clarification, they should speak to their line manager in the first instance.

Use of equipment and materials

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

It is not acceptable to use the school's equipment and materials or an employee's own equipment/materials in the workplace in any of the following contexts:

- Illegal activity
- Activities for personal gain
- Excessive personal messages
- 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
- Accessing sites which could be regarded as sexually explicit pornographic or otherwise distasteful or offensive.
- Racist, sexist or other conduct or messages which contravene the school's employment diversity policies
- Actions which could embarrass the school or bring it into disrepute
- To reply to SPAM
- Non work related business activities eg regular use of on line auctions, newsletters, ebay, etc.

Staff must not carry out personal activities during working hours, nor mix private business with official duties. Official equipment may be used for private purposes as long as such use does not interfere with its use for school business or be used for activities detailed above. School materials may be used for private purposes provided that permission is obtained beforehand from line managers and the finance staff are informed so that full cost payment can be made.

If an employee needs to use the school's phone for private purposes the call should be timed and the appropriate call charge be passed to the finance staff. Payment is not required where employees need to phone to notify someone they have been delayed at work or in other emergencies. In terms of using other equipment and materials, the decision to allow such use is at your line manager's discretion. Using the photocopier for private use would fall into this category.

If given permission, approved acceptable private use should normally take place in the employee's own time but where this is not practicable or sensible, any disruption to the employee's official work or that of colleagues must be minimal. Official work will always take precedence.

E-mail (volume and size in terms of 'KB')

Office systems should not be used for excessive personal use. Some limited internal social e-mail is not problematic e.g. arrangements for an office social event or news of a sick colleague. Staff must not carry out personal activities during working hours, nor mix private with official business, but, on this basis limited external email communication is permitted.

- Personal external e-mail to a staff business account should be discouraged and external contacts should be asked to minimise causing possible embarrassment by not over-doing this.
- Staff should be aware that e-mail is not a private and confidential means of communication and your line manager, can at any time review any of your desktop and e-mail files.
- Sending excessively large attachments decreases the effectiveness of EPCHS's email service and delays communications for all users, it also has a major impact on internal technical resources. Currently restrictions on file size are in place. If you receive a warning please contact the IT Service. Files should be shared via the "Staff Drive" or "Subject Shares" areas.
- Photographs or other large attachments must not be sent for personal or novelty responses.

E-mail (content)

The school uses automated software tools to identify any e-mails containing inappropriate content, usually selecting on words with a sexual / pornographic connotation. Line managers will interview staff whose e-mails are picked up by the "content monitoring" software. If use cannot be justified, disciplinary action is inevitable. The school does not tolerate use of its systems for this type of activity.

Sensitive/Confidential Information

Care should be taken when sending sensitive/confidential information via e-mail. You should alert the recipient in the subject line and send the information as an attachment rather than typed in the body of the e-mail, and check that the recipient's email address is correct before sending.

Internet

Because of the nature of our work, using the Internet is very much second nature and staff have unrestricted access to the Internet for business purposes. Reasonable access for private use which does not affect work duties and the content is not within the context detailed is acceptable.

Private downloads of music files, games, videos etc via the school's network is not permitted.

Streaming of TV programmes or music for personal use is not permitted.

Customisation of home pages to enhance efficient working is acceptable, however software downloads must be approved by the IT Services.

Social Media

School staff should not invite, accept or engage in communications with parents or students from the school community in any personal social media whilst in employment at the school.

School staff should never act in a way that could bring the School into disrepute – even if you are not on duty, for example use of social media and publishing of photographs that might compromise your own reputation as well as that of the school.

Security

Staff have a responsibility for securing access to their IT equipment when leaving their desk. Staff should safeguard their machine when away from the office. Computers should be "locked" (Hold down the Windows key and press "L"). Classrooms containing IT equipment should be supervised at ALL times and locked when a member of staff is not present.

Staff have responsibility to have regard for the confidentiality of passwords and security codes etc connected with their work. Your password should contain letters and numbers, i.e. *l1ke thi5.* These should not be shared. Staff must change their password on a regular basis and will be automatically prompted to do so.

Staff are able to access data and resources remotely from home and should avoid saving data to removable devices. Staff have a responsibility to take particular care that laptops or removable devices which do contain any personal data must not be accessed by other users when out of school. Staff must make sure that any devices taken off site are transported securely for storage in a secure location and not left unattended at any time.

The SLT will take the most serious view of any action or inaction on the part of an employee who deliberately, recklessly or carelessly jeopardises the security of data, records or systems.

Any employee detecting a potential security problem (e.g. a virus or unauthorised access) must immediately take any action within their authorised power to safeguard or resolve the situation e.g. disconnect any infected machine from the network (remove the cable) and notify IT Services immediately.

Every employee must observe the school's communications and information technology security requirements and act responsibly when using equipment and materials. IT Services can provide training to enable staff to comply with this requirement. Please see your line manager in the first instance.

Inadvertent access to inappropriate sites and inappropriate emails

If an employee inadvertently accesses an inappropriate web site, they should leave it immediately but notify IT Services of the incident, giving the date and time, web address (or general description) of 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 (e.g. 'clean jokes'), the recipient should point out to the sender that they do not wish to receive such messages at their workplace because they believe they contravene the school'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 such material and keep a record of doing so.

Monitoring

Monitoring information will not be accessible (or distributed) any more widely than is necessary for the purposes for which it is needed.

All employees should be made aware at induction and at intervals thereafter, that, in relation to any electronic communication, there can be no expectation of absolute privacy when using the school's equipment provided for official/ work purposes; and that the school reserves the right to monitor all communications including their content. This monitoring is carried out to ensure that equipment and systems are used efficiently and effectively, to maintain systems security and to detect any breaches of this policy or the law. Normally monitoring consists of the following:

- **Emails.** Every incoming and outgoing email message is automatically swept for key words which could indicate misuse.
- **Web access.** Access to some web sites is automatically prevented (e.g. pornographic, racist and violent sites) and others are restricted (e.g. MP3 music sites and Web Chat) and a message warns that these types of sites are strictly for business purposes. However, an automatic record is made of all sites visited and a sweep made of site names and content against pre-determined criteria, to identify inappropriate sites together with attempts made to access such sites.

Access to and retention of monitoring information

Access to routine monitoring information is restricted. Regular reports will be produced identifying high usage of communications and information technology and areas where the school may be at risk, e.g. as a result of weak passwords. These will be made available to SLT. If a line manager identifies a potential issue of abuse they will be given access to more detailed information to enable them to decide whether further investigation is necessary and enable appropriate action to be taken. They will respect the confidentiality of all communications and disclose the contents of communications only where there are grounds for suspecting abuse of this policy. Where this is the case, other senior managers may then be involved and are likely to be made aware of the contents of communications.

Reporting misuse

If any employee suspects activity which may constitute misuse or activities which could jeopardise system security, they must report this immediately to IT Services or their Line Manager.

Consequences of breach: Disciplinary action

Breaches of this policy may result in the application of the Disciplinary Procedure and may, if deemed sufficiently serious, be treated as gross misconduct. Police involvement and prosecution may follow if the conduct in question constitutes possible criminal activity.