Review – Autumn 2023

St. Winefride's Catholic Primary

Communications and Information: Acceptable Use Policy

Mission Statement

Welcome to St Winefride's where we come together to learn, laugh, listen, live and love in the presence of Jesus.

At our school, we believe that everyone is valued as a unique gift from God.

We work together to create an engaging learning environment, where all children are challenged to achieve their full potential.

Purpose

The policy has been developed to advise employees of if, when and under what conditions they may use the school's/Council's communications and information systems for personal reasons. It sets standards to ensure that employees understand the position and do not inadvertently use communications and information in inappropriate circumstances.

The school/Council recognises employees' rights to privacy but needs to balance this with the requirement on the school/Council (as a public service) to act appropriately, with probity, to safeguard its business systems, and to be seen to be doing so.

In applying the policy, the school/Council 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

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, e.g.

- mail systems (internal and external).
- internet and intranet (email, web access and video conferencing).
- telephones (hard wired and mobile).
- pagers.
- fax equipment.
- computers – this covers ANY computer used for work purposes, whether at the place of work or elsewhere (see Annex on Laptops For Teachers).
- photocopying, printing and reproduction equipment.
- recording / playback equipment.
- documents and publications (any type or format).

The policy applies to all employees (as a contractual term), agency staff and to other people acting in a similar capacity to an employee. It will also apply to staff of Contractors and other individuals providing services/support (E.g. Volunteers). It takes account of the requirements and expectations of all relevant legislation.

The Headteachers will discuss the policy with their teams and agree parameters within which staff members will act. Every employee will have the policy explained to them at induction, and be given a copy for future reference. If at any stage employees require further clarification, they should speak to their Headteacher in the first instance.

Where an employee needs to discuss personal information with Occupational Health, HR or their Trade Union, they will be given privacy to do this. Headteachers will agree with Trade Union representatives the arrangements for using school communication and information systems which will be provided in accordance with trade union facilities agreement and the ACAS Code of Practice.

Use of Equipment and Materials

Use of Facilities
The school's/Council's Code of Conduct for Officers states that staff must not carry out personal activities during working hours, nor mix private business with official duties. Official equipment and materials should not be used for general private purposes without prior permission from the Headteacher.

Facilities for Private Use
School laptops are provided for nominated teaching staff related to school business.

Telephones (landline) are available for some private calls. These should be used outside teaching time, unless there is an emergency or other urgent need. It is not always possible to guarantee complete privacy because of the location of the telephones. Payment is not required where employees need to contact someone in order to notify them that they have been delayed at work or in other emergencies. (Payment may be requested, depending upon duration and destination of telephone call.)

In terms of using other equipment and materials, the decision to allow such use is at the Headteacher's discretion. However, the following are provided as examples to illustrate where it might be reasonable for permission to be given for reasonable use for private purposes, under the conditions shown and after getting prior approval.

- Social or recreational activities associated with school employment.
- Regular activity for a legitimate voluntary body or charity.
- Training or development associated with employment.
- Occasional and brief essential family communications or other personal messages.

The Headteacher may veto private use at any time if they consider that circumstances justify this in general or particular cases, e.g. because of improper use or over-use. A charge may be made for materials if the values are significant.

In emergencies permission might need to be obtained retrospectively or again this may be covered by the general parameters agreed with the team.

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.

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 Code of Practice.

It is not acceptable to use 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 private gain.
- Personal shopping.
- Excessive personal messages.
- Playing games (except those games pre-loaded as part of the Microsoft programme suite, which may be accessed in the employee's own time).
- 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.
- Random searching of the web.
- Accessing sites which could be regarded as sexually explicit pornographic or otherwise distasteful or offensive.
- Using message encryption or anonymised web search, except where encryption is required for official school business purposes.
- Racist, sexist or other conduct or messages which contravene the Council's employment diversity policies.
- Actions which could embarrass the school or bring it into disrepute.

GDPR

New regulations have been implemented following the **General Data Protection Regulation** (**GDPR**) coming into force on May 25, 2018. All staff are now aware that:

- All memory sticks that hold any confidential information or information that could identify persons in the workplace and/or, school, are to be encrypted.
- All devices, such as laptops, are to be password protected.
- They must only transport, hold, disclose or share personal information about themselves, other staff members, pupils or their parents, as outlined by the school GDPR Policy.
- They must ensure that, where data or confidential information is electronically transferred outside the school network, it must be encrypted using the Egress software.
- The use of personal cloud based online storage must not be used to store, share or access any school related personal data.
- The use of personal email addresses by governors or staff is not allowed. It is also advised that staff are also not to correspond with governors via anything other than a school email account.

Inadvertent access to inappropriate sites and emails

If an employee inadvertently accesses an inappropriate web site, they should leave it immediately but notify their school 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 Headteacher. If the emails are racist or sexist or could otherwise be regarded as offensive, they should be left in the inbox and the Headteacher notified immediately. Employees should notify the sender that they do not wish to receive further such material and keep a record of doing so.

School/Council 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, at intervals thereafter and possibly through automatic messages on school/Council equipment, that, in relation to any electronic communication, there can be no expectation of absolute privacy when using school/Council 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:

- **Telephones and fax -** The school reserves the right to monitor communication content selectively if abuse is suggested. However such monitoring would only take place following an assessment that such steps are necessary to further a particular investigation or concern. It would only be authorised following the advice of the Council's Statutory Officers. Where calls are made via the Cheshire West and Chester network, an automatic record is kept of every number called, from where and the duration of the call. Further action is taken where particular numbers called or the frequency and duration of calls suggest abuse of this policy.

- **Emails -** When using the Cheshire West and Chester network, every incoming and outgoing email message is automatically swept for key words which could indicate misuse.

- **Web access -** When using the Cheshire West and Chester network, 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. The school reserves the right to apply similar restrictions and screening to its own web access systems.

- **Mail -** The privacy of internal and external postal communications marked 'personal' will normally be respected (unless abuse of this policy is suspected) but all other communications may be opened for good reason by a Headteacher, Admin. Officer or colleague.

Access to and retention of monitoring information

In the case of Cheshire West and Chester systems, access to routine monitoring information is restricted to specified employees in Information & Communication Technology Services and Audit. If they identify a potential issue of abuse the relevant Headteacher will be given access to the information to 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.

Surveillance

Covert monitoring will only be used in connection with a criminal investigation or where abuse of terms of employment, e.g. sickness scheme, is being investigated. This will always be in accordance with the statutory safeguards applicable to such activity (the Regulation of Investigatory Powers Act and the Human Rights Act) only authorised following careful consideration of the need for such action in accordance with 'Surveillance under the Regulation of Investigatory Powers Act 2000'.

Security

Every employee must observe the Council's communication and information technology security requirements (as detailed in IT Code of Practice) and act responsibly when using equipment and materials. Employees will be provided with the necessary briefing and training to enable them to comply with this requirement. Headteachers 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 records of systems. Any employee detecting a potential security problem (e.g. a virus or unauthorised access) must immediately take 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 the ICT helpdesk.

Reporting misuse
If any employee suspects activity which may constitute misuse or activities which could jeopardise system security, they must report this immediately to Headteacher or use the Whistle-blowing Policy. The Headteacher must consider whether it would be appropriate to involve Internal Audit and must always ensure that all relevant records and documents (paper and electronic) are safeguarded and retained securely.

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. In case of supply staff, volunteers etc. breach may result in termination of the contract or relevant arrangement and/or withdrawal of the relevant facility. Police involvement and prosecution may follow if the conduct in question constitutes possible criminal activity.

Agreed by Policies' Committee – 09.11.21

GDPR Compliant – Communication and Information Acceptable Use Policy

I can confirm that I have received and read the school Communication and Information Acceptable Use Policy and agree to adhere to it. I confirm that I understand the restriction on the use of personal accounts and the downloading of personal data.

Signed_____ Name_____

Date_____