IT SECURITY POLICY

This policy applies to employees of the Parish Council, and Freeland Parish Councillors who use personal computers as part of their parish duties.

Freeland Parish Council encourages the use of email and the internet at work where this can save time and expense. However, it requires that employees and Councillors follow the rules laid out in this policy. If an employee or Councillor is unsure about whether something they propose to do might breach this IT Security policy, they should seek advice from the Chairman immediately.

1. Employees and Councillors must never intentionally download any offensive, irrelevant or inappropriate information or send email messages which could be interpreted as discriminatory on the grounds of race, gender, hair colour, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs or national origin, or which might amount to harassment on any of these grounds.
2. Emails that employees or Councillors intend to send should be checked carefully. Email should be treated like any other form of written communication and, as such, what is normally unacceptable in a letter is equally unacceptable in an email communication.
3. The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be treated as misconduct. In serious cases this could be regarded as gross misconduct and could therefore lead to termination of employment/office.
4. If an employee or Councillor receives an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, they should not forward it to any other address.
5. The Council encourages employees to become familiar with the internet and does not currently impose any time limitation of work-related internet use. It trusts employees not to abuse the latitude given to them, but if this trust is abused the Council reserves the right to alter this policy in this respect.
6. The Council reserves the right to monitor employee's emails, but will endeavour to inform an affected employee when this is to happen and the reasons for it.
7. As the Council increasingly relies on information stored on a PC, much of which is valuable and difficult to recreate, important or sensitive computerised data must be protected from corruption, distribution or unauthorised disclosure. The Parish Council computer must be password protected and have adequate and up to date anti-virus software installed and back-up procedures in place. This includes the swapping of data storage media such as memory sticks that are loaded with the most up to date data with a nominated and agreed officer of the Council at the beginning of each month to ensure an off-site record is kept in case of fire or flood damage at the normal records site.
8. All reasonable steps much be taken to protect the Parish Council's data, including filing cabinets being kept locked when not in use wherever possible.
9. Passwords must not be disclosed to any other third party and should be changed regularly. Passwords should be changed immediately if any suspicion arises that a password has become known to anyone other than the intended user.

This policy may be reviewed at any time and any changes that are deemed necessary will be made as appropriate.

Approved by Council: March 2010