EASTINGTON PARISH COUNCIL

INFORMATION SECURITY POLICY

INTRODUCTION

This policy sets out the Parish Council's position of the use of the Internet, email and other Parish Council computer systems and data contained therein. Any deliberate breach of this policy will be dealt with under the Disciplinary Policy.

Internet Usage

The use of the Internet by staff is permitted and encouraged where such use is part of the normal execution of an employee's job responsibilities. The Internet is to be used in a manner that is consistent with the Parish Council's standards of conduct. Any information (including email messages) that has been down loaded from the Internet by whatever means should be checked for computer viruses before being loaded onto the Parish Council laptop. This policy is necessary in order to avoid the Parish Council's information systems being subjected to computer hacking and software viruses.

Appropriate Usage

The Parish Council's computer connections are to be used for the Parish Council's business/provision of services. Connections to the Internet must only be via IT equipment authorised for the purpose. There is no automatic right to use email for personal use even if it is paid for. The Parish Council reserves the right to periodically examine Parish Council's own computer equipment, directories, files and their contents to ensure compliance with the law and with Parish Council policies.

Non-permitted Usage

The following is not allowed. This list is not exhaustive:

- Downloading any software or electronic files without the required virus protection measures in place
- Making or posting indecent remarks and proposals
- Visiting Websites that contain obscene, hateful or other objectionable material or distributing and forwarding such material
- Soliciting for personal gain or profit
- Gambling
- Conducting illegal activities
- Hacking, ie attempting unauthorised access into or intentionally interfering with any Internet/Intranet gateway/system/server
- Uploading/downloading commercial software in violation of its licence agreement
- Receiving newsgroup emails that are unrelated to the business of the Parish Council.
- Be careful not to fall for phishing scams that arrive via email or on your social networking pages, providing a link for you to click, leading to a fake login page.

Security

All information received/retrieved over the Internet must be authenticated and / or validated before being used in the services of the Parish Council. All staff must report Internet security weaknesses that they become aware of to the Parish Clerk or the Chair of the Council. The distribution of any information through the Internet, the Web, computer-based online services, email and messaging systems is subject to the scrutiny and approval of the Parish Council, which reserves the right to determine the suitability and confidentiality of information disseminated.

Virus Protection

The world wide web and email are high risk sources of computer virus infections. It is essential that all material received over the Internet and via email is checked before use or distribution. In particular, email attachments must be virus checked before distributing further. Viruses that are detected must be reported to the Parish Clerk or the Chair of the Council. The Parish Council also has the responsibility not to distribute viruses. Consequently items dispatched over the Internet must be checked to ensure that they are virus free. The final responsibility for virus checking will always remain with the user.

Passwords

Laptop and email passwords are to be changed every six months and must contain at least 1 capital letter and 1 numerical character to ensure the passwords are "strong". The passwords will be known only to the Parish Clerk and Chair of the Council.

Information Disclosure Rules and Individuals Liability

Members of the Council and staff are prohibited from revealing or publicising proprietary, confidential or personal information that they have not been specifically authorised to do so. Such information includes but is not limited to:

- Financial information not already publicly disclosed through authorised channels
- Personal information
- Operational information
- Information provided to the Parish Council in confidence or under a non-disclosure agreement
- Computer access codes and similar or related information that might assist unauthorised access
- Legal proceedings
- Information that might provide an external organisation with a business advantage
- Computer programs
- Databases and the information contained therein.