Harrietsham Parish Council

Internet Usage Policy

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 Council's standards of conduct. Any information (including email messages) that has been downloaded from the Internet by whatever means should be checked for computer viruses before being loaded on to any machine which is connected to the Parish Council's network. This policy is necessary in order to avoid the Parish Council's information systems being subjected to computer hacking and software viruses.

Appropriate Usage

Connections to the Parish Council's internet are to be used for Council business and the provision of services only. Connections to the internet must only be via IT equipment authorised for the purpose. This equipment must be operated by authorised Parish Council staff, except where access has been specifically sanctioned for use by other members of staff/service providers. There is no automatic right to use email for personal use even if it is paid for.

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 i.e. attempting unauthorised access into or intentionally interfering with any Internet/Intranet gateway/system/server.
- Uploading/downloading commercial software in violation of its copyright
- Receiving list serve (newsgroup) emails that are unrelated to the business of the Council.
- Sending electronic "chainletters".

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 Clerk. The distribution of any information through

the Internet, the Web, computer-based on-line 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 internet is a high-risk source of computer virus infection. Thus, it is essential that all material received over the Internet is checked before use or distribution. In particular, all email and attachments must be opened and checked before storing and distributing further. Viruses that are detected must be reported to the Clerk. The 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.

Information Disclosure Rules and Individual Liability

Staff are prohibited from revealing or publicising proprietary, confidential or personal information via the Internet 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.
- Client information.
- Operational information.
- Information provided to the Parish Council in confidence or under anon disclosure agreement.
- Computer and network 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.