BREDGAR PARISH COUNCIL (BPC)

Information Security and Information Technology (IT) Procedure

This Procedure was reviewed by the Full Council at its meeting held on 29th August 2018.

1) **Scope**
   Staff and Councillors using BPC or their own IT equipment are required to read this procedure.

2) **Objective**
   To prescribe the security and IT procedures that staff and councillors should operate as they implement BPC Policies.

3) **Procedure**
   The BPC computer will be held by the Clerk for conducting council business and storing council data.

   Councillors use their own computer equipment and networks. If they store council data on their own equipment it is strongly recommended that they adhere as closely as possible to this procedure.

4) **Security – BPC equipment**
   The BPC computer must be installed with a supported operating system. I.E. An operating system that is being kept secure by regular security updates.
   Secure access to the computer will be by a unique userid and a password. The password must be at least 8 characters, include letters (upper and lower case), numbers and other characters. Userid and passwords must not be shared.
   Security Updates must be installed regularly and in a timely manner.
   Anti-Virus Software must be installed and regularly updated.
   A firewall must be active on the computer to protect against malicious attacks from any network.
   Council data stored on the computer must be held in an encrypted folder.

   The Clerk of BPC will pass userid, password details, for the computer account and encryption, to the Chair of BPC in a sealed envelope after each password or account change.

5) **Security – BYOD equipment**

   If BPC staff and councillors store council data on their BYOD equipment it is strongly recommended that they apply the same security as that indicated for BPC equipment in

Section 4 of this procedure.

Instructions for use of encryption can be found in the Encryption Work Instruction.

BPC staff or councillors must inform the Data Protection Compliance Officer and the Chair if their BYOD equipment has been subject to a malicious attack and / or data breach.

6) **Backup**
Council data will be backed up regularly to an encrypted folder on an external USB storage device. The storage device to be stored in a different location to the computer. E.G. If the Clerk keeps the computer at home, the BPC Chair or Vice Chair would hold the backup USB storage device.

It is recommended that a number of USB Storage devices are used for backup. This will enable the clerk to always have a returned device for the next backup and will protect against device failure.

In addition, all published council data will be stored on the BPC website, as soon as possible, to act as a secondary backup.

7) **Email**
It is strongly recommended that BPC staff and councillors set up and operate separate email accounts for council business. BPC staff and councillors are expected to use an Internet hosted email account and to rely on the backup and recovery capabilities of those providers.

It is recommended but not mandatory that emails account names are in the form of :

“bpc.<role or surname>@<email provider>”