Bollington
TOWN COUNCIL

INFORMATION SECURITY POLICY

PRINCIPLES & PURPOSE

This Policy sets out the Council's commitment to information security within the Council and provides clear direction on responsibilities and procedures. This policy should be implemented in conjunction with the Council's Data Protection, Communications and Data Retention Policies.

Bollington Town Council is a Data Controller, as defined under the General Data Protection Regulations 2018, and has registered as such with the Information Commissioner's Office.

PROTOCOLS

System Security Processes and Procedures

The Council will provide and maintain security processes and procedures for all key information systems. The procedures will uphold the principles of confidentiality, integrity, availability and suitability and be assessed for their impact upon other systems and services.

The security procedures will provide preventative measures to reduce the risks to the system, the information held within the system and the service it supports.

A Continuity plan will be developed and maintained for each system to ensure the principles are sustained and enable the continuation of services following failure or damage to systems or facilities.

The Clerk will be responsible for the implementation and promotion of the procedures.

Physical Security

Adequate and practical access controls will be provided in all areas in which personal and business data is stored or used. Unattended rooms should be secured at all times with locked doors as a minimum security requirement.

All documents disclosing identifiable information will be transported in sealed containers eg envelopes. Staff and Members should ensure that any such printed material produced or taken off the Council premises should be kept to a minimum, stored securely and returned for disposal within an acceptable timescale according to the Data Retention Policy.

Within their level of authority, staff will be responsible for minimising the risk of theft or vandalism of the data and equipment through common-sense precautions. In particular high value equipment such as, laptop computers, should not be left unattended or unsecured and paper records should not be left in public view.

The physical environment in which data and equipment is stored will be suitable and fit for purpose to ensure the safety of the data and equipment.

Digital Security

Bollington Town Council uses encrypted Microsoft 365 technology to process and store data.
This provides a high level of security when used in compliance with the key points below.

- The SharePoint and data storage administration and permission levels must be appropriately managed to protect against unauthorised access to documents.
- Staff and Councillors must use the Bollington-tc.gov.uk 365 account assigned to them for all Council business and communications.
- Staff and Councillors must not disclose their password to anyone else, or use another person's log in into the system.
- Passwords will be changed every 3 months and set according to strictly controlled criteria.
- Computers within the office environment must be password protected and screen locked when unattended.
- Council owned hardware will be protected by suitable anti-virus software and will be kept updated with all the latest security downloads.
- Computer users have responsibility for the security of the equipment in their care and shall not commit an act to compromise the data or Information Security Policy.
- Where staff use syncing technology in OneDrive special consideration will be given to the types of data sync'd locally, and whether extra security such as file password protection will be required.
- Councillors and staff need to be aware of any personal data they keep within their own BTC OneDrive accounts and be mindful that they need to have a legal basis to retain that data. If unsure then they must take advice from the Clerk or the DPO.
- It is good practise to send documents as links within the 365 system rather than as email attachments. This way, if required, access can be denied to the data at source, or the data destroyed with the confidence that there are not multiple copies to account for.

Offsite Hardware Data Security

- Where staff or Councillors wish to use their own PCs or laptops off-site these machines must be protected with suitable up to date virus software and password protected.
- A screen lock must be activated when the machine is unattended.
- Office 365 accounts must never be left logged in where a machine is shared with or could be accessed by anyone else.
- Council Information must not be downloaded onto the hard drive of any personal device – instead Councillors and staff are provided with 1Tb online storage in the form of OneDrive.

BOYD*

Bollington Town Council will provide a portable tablet device to Councillors on request. These devices are specifically for Council Business and not to be used for any other purpose. No software is to be downloaded by the user without the permission of the clerk.

However, some Councillors and staff will find that the use of “BOYDs” is more satisfactory and the following key points must be followed in addition to the general points outlined previously.

**What is a BOYD?*
1. Consumer electronic devices such as smart phones and tablet computers have seen a huge rise in popularity, available features and capability. This might mean that individuals’ own devices are used to access council information.

2. This trend is commonly known as ‘bring your own device’ or BYOD.

3. Permitting a range of devices to process personal data held by an organisation gives rise to a number of questions a data controller must answer in order to continue to comply with its data protection obligations. It is important to remember that the data controller must remain in control of the personal data for which he is responsible, regardless of the ownership of the device used to carry out the processing.

- Staff and Councillors using tablets and smartphones must ensure that the device is kept secure with an up to date virus checker where appropriate.
- Portable devices must be password/pin/face recognition protected and must be set to return to the lock screen within a short period of inactivity.
- 365 accounts must never be left logged in on devices which can be accessed by a third party.
- Be aware of network security when using portable devices and avoid using open networks to access 365.

Copyright and licences
The Clerk is responsible for ensuring all computer software packages and non-electronic media for use within an information environment are used in accordance with the terms and conditions of use as set out in the licence agreement.

Disposal and movement of equipment and media
Any media or IT equipment disposed of by the Council will not contain any data or codes that could allow an individual to be identified from it. The disposal of equipment will be made under a controlled and documented environment satisfying the requirements of the General Data Protection Regulations 2018. The disposal of media such as disks and memory sticks must ensure that data cannot be recovered. Disposal of such media through the "everyday" waste collection is not permitted. The Council will implement processes to ensure appropriate disposal of such media.

An inventory of all Council computer equipment will be maintained. Details of any equipment or media disposed of or relocated (other than portable equipment) must be recorded.

Removable Storage Media

Councillors and staff need to be aware of the risks of transporting documents on removable media such as portable hard drive and USB flash drives.

- Downloading of Council documents from within the secure 365 system to a removable media device is prohibited
- The use of 3rd party removable devices to transfer information to Council Computers is prohibited. NB For 3rd party printing purposes there is a USB port on the photocopier.
-

Staff and Councillors' Responsibilities

The Council will make every reasonable effort to ensure that staff and councillors are aware of their responsibilities for the security of information. However, each councillor or member of staff is responsible for ensuring that Security Policy is adhered to and report any breaches of security.

Incident Reporting

Any incidents affecting security must be reported to the Clerk as quickly as possible.

Any Staff Member or Councillor who suffers the loss or theft of a portable device used for Council business must if possible change their 365 password as soon as the loss is noticed and inform the Clerk immediately.

Any Staff Member or Councillor who considers it possible that any device which has been used for Council business may have been compromised by a virus, hackers or any other means must if possible change their 365 password as soon as the loss is noticed and inform the Clerk immediately.

The Clerk will if necessary contact the IT service provider and take appropriate advice from the DPO on any further steps required.

Adopted:
8th May 2018