FILEY TOWN COUNCIL

Laptop & Mobile Device Policy

1. Introduction

Laptops, tablets and smart phones are versatile, portable and highly desirable devices. As a result, this type of device is at greater risk of theft, both for the device itself and as has been noted more recently, for any data that may be held on it. This document is intended to ensure that a person allocated a laptop, tablet or other mobile device understands the associated risk and assumes the appropriate level of responsibility for Filey Town Council's property.

2. Scope

The scope of this policy covers all employees (full time, temporary or contract staff) and all Members of the Town Council who use laptops, tablets and smart phones provided by Filey Town Council.

3. Security Risk

Laptops, tablets and mobile phones are vulnerable to loss and theft due to their portability and small size. Thieves may target these devices both on the Filey Town Council's premises and also whilst in transit. Although the majority of thefts will be carried out in order to resell the device for a quick profit, a significant number of laptops or other mobile devices are stolen for the (sensitive) data they may hold. Such information, if revealed, may cause embarrassment, have a negative impact on the reputation of the Town Council and may result in financial, commercial or competitive loss to the Town Council.

4. User Responsibility

4.1 General rules

- Laptops, tablets and other mobile devices **must** be protected by a strong password (to include numbers and uppercase and lowercase letters) or pin code. All passwords should be held in a central location with the Town Clerk and any change of password should be notified to the Town Clerk.
- Laptop or other mobile device users **must** take shared responsibility for the security of their equipment.
- Any laptop or other mobile device(s) issued to staff remains the property of Filey Town Council.
- Upon leaving employment or changing to a new role where the laptop or other mobile device is no longer required, the member of staff or member of the Town Council **must** return the laptop or mobile device to the Town Clerk or in his/her absence Deputy Town Clerk.
- Before installing software onto mobile devices, staff and members should contact the the Town Clerk for authorisation. Where possible, installations should be carried out by technical staff. When installing applications on mobile devices, it is recommended that only official stores are used e.g. App Store, Google etc.
- Use of unlicensed software is illegal and puts Filey Town Council at significant legal risk.

- Users are specifically prohibited from changing security settings or amending configuration files on any laptop or mobile device issued to them. This includes disabling passwords, pin codes and any installed security programs (e.g. Anti-Virus applications).
- In the event that a laptop or other mobile device is stolen, the user must notify the police and / or any other appropriate authority. It is the user's responsibility to obtain a crime reference number and to inform the Town Clerk as soon as possible after the event.
- Loss of data or information caused by disregarding the recommendations made in this document shall be the sole responsibility of the user of the laptop or mobile device.
- The Council's e-mail and Internet Systems are for use in the effective delivery of the Council's Services and should be used as such.
- **All Council users are required to refer themselves to the Town Council's Information Technology and Electronic Communications Security Policy for detailed guidelines regarding the safe use of internet and electronic communications and please note that this policy is to be read in conjunction with those guidelines.**

4.2 Physical Security

Apart from the financial cost associated with replacing a stolen laptop or mobile device there are associated hidden costs. These include loss of productivity, data replacement, increased insurance premiums and so on. All Filey Town Council laptop or mobile device users are therefore encouraged to take the following physical security measures to prevent the theft of laptops, other mobile devices and sensitive information.

- Laptops, tablets and mobile devices **must not** be left in full view in a vehicle even for a short period of time. Laptops, tablets and mobile devices must be locked in the boot.
- Laptops, tablets and mobile devices **must not** be left in a vehicle overnight, even in a locked boot.
- When leaving a laptop, tablet or mobile device un-attended for an extended period of time, the laptop, tablet or mobile device **must** be kept securely. It **must not** be left out at any other location or office over-night.
- Laptops, tablets or mobile devices **must never** be left unattended in public places even for a very short period of time.

4.3 Access control and Data Protection

- All Filey Town Council users **must** use a password or pin code in order to protect information held on a laptop or mobile device.
- All computer screen displays, including laptops, **must** be locked with the password protected screen saver when left unattended.
- When working in public places such as restaurants, hotel lobbies, on trains or aircraft, care should be taken to prevent others from being able to view potentially sensitive information. The use of Privacy Filters is recommended for these circumstances as these reduce the viewing angle of the screen and prevent casual observers from being able to see sensitive information on the screen. Loss of sensitive data or information could materially damage Filey Town Council.
- Any changes made to files (or data) normally stored on the Town Council's shared (or personal) drives whilst not connected to the Council's Network should be copied back to the normal storage location at the next opportunity. This will reduce the risk of losing information following a physical failure of the device.

Reporting the loss or theft of a Mobile Device

Any loss or theft of a Filey Town Council supplied mobile device (laptop, tablet, mobile phone, external hard disk etc.) **must** be reported to the police and a crime incident / reference number obtained. This should be done immediately after the loss or theft has been discovered. Once the crime reference number has been obtained, the loss or theft **must** be reported to the Town Clerk. If the loss or theft occurs outside of normal operating hours, notification must be made on the next working day following the event. If a mobile phone is lost or stolen, the event **must** be reported to the Town Clerk immediately who will block the number and arrange for a replacement handset to be issued. This should be done before contacting the police and will minimise potential costs associated with misuse.

5. Do's and Don'ts

- **Do** create and use a password or pin code to prevent unauthorised access to the laptop, tablet or other mobile device.
- **Do** take care when connecting the network cable and seating the laptop on docking stations as the connections can be easily damaged.
- **Do** turn your laptop, tablet or mobile device off and put it in an appropriate carrying case when travelling.
- **Do** keep all drinks and any other liquids away from your laptop, tablet or mobile device. Any spillage on the device can result in data loss and expensive repairs.
- **Do** avoid turning off your laptop when the hard disk light is on. This can result in data corruption and / or data loss.
- **Do** make sure that you always copy back any amended documents or data files to your departmental shared folder after working remotely.
- **Do** report a loss or theft as soon as possible after the event.
- **Do** use a Privacy Filter if working in a public place (e.g. on a train, airplane or in a hotel lobby).
- **Don't** subject the laptop, tablet or mobile device to extreme temperature changes (i.e. don't use or store near radiators or fan heaters). Mobile devices are designed to work within a defined temperature range so exposing them to extreme temperatures (highs or lows) may cause the device to malfunction or behave unpredictably. Avoid using laptops in temperatures over 50°C.
- **Don't** leave the laptop or other mobile device unattended. If you need to leave your desk, put the laptop, tablet or mobile device in a lockable drawer or take it with you. Lock your office door.
- **Don't** use your laptop, tablet or mobile device for accessing sensitive Town Council related information in public places if there is a possibility that the information could be viewed by unauthorised individuals and hence lead to information theft.

6. Violations and Penalties

Violation of this policy may result in disciplinary action.

7. Other Council Policies

This policy is read in conjunction with the Town Council's Electronic Communications Policy.

ADOPTED 23 May 2018
REVIEWED 6 May 2020 & May 2021
To be reviewed May 2022