Blackwell Parish Council

Mobile Device Policy (for Council supplied equipment)

Date approved:	Review Date:

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 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 risk and assumes and appropriate level of responsibility for Blackwell Parish Council property.

2. Scope
The scope of this policy covers all employees (full time, temporary or contract staff) and all Members of Blackwell Parish Council who use laptops and smart phones provided by Blackwell Parish 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 Blackwell Parish 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 Blackwell Parish Council and may result in financial, commercial or competitive loss to the Parish Council.

4. User Responsibility
4.1 General Rules
a. Any laptop or other mobile device(s) issued remain the property of Blackwell Parish Council.
b. When issued with a mobile device, the user will be asked to sign to confirm receipt and that this policy has been read and understood.
c. Laptops or other mobile device users must take shared responsibility for the security of their equipment.
d. 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 Clerk and any change of password should be notified to the Parish Clerk.
e. 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 Parish Council must return the laptop or mobile device to the Parish Clerk.
f. Before installing software onto mobile devices, staff and members should contact the Parish Clerk for authorisation. When installing applications on mobile devices, it is recommended that only official stores are used: for example, App Store, Google, etc.
g. Software must be licensed.
h. 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 programmes: for example, Anti-Virus applications.
i. 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 Parish Clerk as soon as possible after the event.
j. If a mobile phone is lost or stolen, the event must be reported to the Parish 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.
k. 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.
l. 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.

m. Do turn your laptop, tablet or mobile device off and put it in an appropriate carrying case when travelling.
n. 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.
o. Do make sure that you always copy back any amended documents or data files to the shared folder after working remotely.
p. 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.

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 Blackwell Parish 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.

a. Laptops, tablets and mobile devices must not be left in full view in a vehicle even for a short period of time.
b. Laptops, tablets and mobile devices must not be left in a vehicle overnight, even in a locked boot.
c. 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.
d. 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

a. All Blackwell Parish Council users must use a password or pin code in order to protect information held on a laptop or mobile device.
b. All computer screen displays, including laptops, must be locked with the password protected screen saver when left unattended.
c. When working in public places, care should be taken to prevent others from being able to view potentially sensitive information. Loss of sensitive data or information could materially damage Blackwell Parish Council.
d. Any changes made to files (or data) normally stored on the Parish 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.

5. Violations and Penalties

Violation of this policy may result in disciplinary action.

To be reviewed annually.

This policy is fully supported by the members of Blackwell Parish Council	
Signed by	Chairman, Blackwell Parish Council
Date	