CLAPHAM PARISH COUNCIL

'BRING YOUR OWN DEVICE' POLICY

INTERPRETATION

In this policy:

'Devices'	means computers (desktop and laptop), tablets, smartphones and external hard drives.
'Parish Council Business'	means any activity undertaken in the role of member or employee of the Parish Council.
'**Personal Data**'	has the meaning set out in Article 4(1) of the General Data Protection Regulation: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"
'Personally owned'	means ownership of a Device by a person or legal entity which is not the Parish Council.

1. PURPOSE

The purpose of this policy is to ensure so far as possible that personally owned Devices used by Councillors and the Clerk to conduct Parish Council Business are used in a manner which protects Personal Data.

2. RISKS

The Parish Council has identified the following risks inherent in using personally owned Devices to conduct Parish Council Business:

Event / Action	Risk
Inadequate or lack of appropriate security measures used to control access to Device	Personal Data may be accessible to third parties
Device used in an insecure manner	Device could be affected by malware which could result in Personal Data being accessed by third parties
Device lost or stolen	Personal Data may be accessible to third parties
Device sold or given away	Personal Data may be accessible to third parties unless Device appropriately cleared before transfer by restoring factory settings
Clerk ceases to be employed by the Parish Council or Councillor ceases to be a member of the Parish Council	Personal Data may remain accessible via the Device and could be used for unauthorised purposes or disclosed to third parties

3. ACCESS TO DEVICES

3.1 Devices used for Parish Council Business must be secured by a password, PIN or a biometric access control such as fingerprint recognition.

3.2 Passwords or PIN must comply with the following rules:

(a) Passwords or PIN should not be written down.

(b) A different password or PIN should be used for each and all Devices or email accounts.

(c) Passwords or PIN must not be disclosed to any other person. If a password is disclosed to any other person, whether deliberately or inadvertently, it must be changed immediately.

(d) Passwords or PIN should be changed at least every 12 months.

(e) Passwords should comprise a mix of letters, numbers and symbols, at least 8 characters long.

3.3 Devices must be configured to automatically lock if left idle for more than five minutes in the case of smartphones, tablets or laptops and ten minutes in the case of desktop computers.

4. SAFE USAGE OF DEVICES

4.1 Devices must have appropriate and up to date anti-virus and anti-malware software.

4.2 Home Wi-Fi networks must be encrypted.

4.3 Care should be exercised if using public Wi-Fi to connect Devices.

5. RETENTION AND USE OF PERSONAL DATA

5.1. Personal Data received for the purposes of Parish Council Business and accessed via a personally owned Device must be permanently deleted from the Device or email account once the related Parish Council Business is completed.

5.2. Personal Data should not be retained on a Device or in an email account in case it is needed for a different purpose in the future unless permission has been obtained to retain the data for general Parish Council Business or unless the Parish Council is

required by law to retain the Personal Data.

5.3. Personal Data must not be used by any person for any other purpose than that for which it has been provided.

5.4. Personal Data received for the purposes of Parish Council Business must not be shared with any other person or organisation.

6. LOST OR STOLEN DEVICES

In the event that a Device is lost or stolen, or is suspected of having been lost or stolen, the Chair and Clerk of the Parish Council must be informed. The Parish Council will work with the owner of the lost or stolen Device to identify any personal data at risk and will then take appropriate action, including reporting any breach to the ICO, as necessary.

7. REPAIR OF DEVICES

If a Device needs to be repaired, the owner will take all reasonable steps to ensure that the repairer cannot access any Personal Data.

8. TRANSFER OR DISPOSAL OF DEVICES USED FOR PARISH COUNCIL BUSINESS

If the owner wishes to transfer or dispose of a Device which has been used for Parish Council Business all Personal Data must be deleted from that Device using a method which prevents recovery. Any email accounts used by the Councillor or Clerk for Parish Council Business should be deleted from the Device.

9. LEAVING THE PARISH COUNCIL

If a Councillor ceases to be a member of the Parish Council for any reason: (a) all Personal Data received in the course of Parish Council Business must be permanently deleted from Devices and from any email account used for Parish Council Business; and (b) all hard copies should be shredded or passed to the Clerk for destruction.

On the termination of the Clerk's employment by the Parish Council: (a) the Clerk must return Devices issued by the Parish Council immediately; and (b) all Personal Data or other information received in the course of Parish Council Business must be permanently deleted from personally owned Devices.