# INFORMATION SECURITY POLICY

**Approved by Council:** **October 2024**

**Date to be Reviewed:** **April 2025**

## 1. Principles and Purpose

This Policy sets out the Council's commitment to information security within the Council and provides clear direction on responsibilities and procedures.

Offa Community Council is a Data Controller, as defined under the General Data Protection Regulation (GDPR) and has registered as such with the Information Commissioner's Office.

## 2. Protocols

### 2.1 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, 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.

The Council will apply controls to comply with the General Data Protection Regulation.

A Continuity plan is available to support 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.

### 2.2 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 always secured with locked doors as a minimum-security requirement.

All documents disclosing identifiable information will be transported in sealed containers e.g. envelopes.

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. 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.

## 2.3 Logical Security

All computerised information and systems must be regularly backed up to a secure environment.

All computerised information systems will be password controlled and all passwords will be treated with the strictest confidence and users will not divulge their password to any unauthorised person. All sensitive data will be password protected.

## 2.4 Copyright and Licenses

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.

## 2.5 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 Regulation. 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.

## 2.6 Personal Computers

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.

Computer users will be made aware of their responsibilities through this policy and the BYOD Policy.

## 2.7 Staff and Councillor's 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 the Information Security Policy is adhered to and report any breaches of security.

## 2.8 Incident Reporting

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