OFFA COMMUNITY COUNCIL

INFORMATION SECURITY POLICY

Information is essential to delivering services to citizens and businesses. Information security refers to the defence of information or information systems from unauthorised or unintended access, destruction, disruption or tampering.

It is important that the Council acts appropriately with the information we obtain, store and process.

Confidentiality, integrity and availability of information must be proportional and appropriate to maintain services, comply with relevent legislation and provide trust to our customers and partners.

Application of policy

Everyone who accesses information the Council holds must be aware of these policy statements and their responsibilities in relation to information security.

Offa Community Council commits to informing all employees, voluntary workers, agency staff, contractors, Councillors and other third parties of their obligations before they are authorised to access systems and information and subsequently at regular intervals.

Other organisations, and their users, granted access to information held by Offa Community Council must abide by this policy.

This policy should be read in conjunction with the Data Protection policy.

All those who access information may be held personally responsible for any breach or misuse.

Information security principles

Information security is the preservation of:

Confidentiality – ensuring that information is accessible only to those authorised to have access

Integrity – safeguarding the accuracy and completeness of information and processing methods

Availability – ensuring that authorised users have access to information and associated assets when required.

Roles and responsibilities

The Council ensures compliance with laws governing the processing and use of information.

The Clerk to the Council acts as Accountable Officer ensuring that all information is appropriately protected:

Ensure they delete or disable all identification codes and passwords relating to members of staff who leave the employment of the Council on their last working day

Ensure that written backup instructions for each system under their management are produced. Backup copies should be held securely.

Ensure systems are protected from external attack

Ensure that employees are fully conversant with this policy and all associated standards, procedures, guidelines and relevant legislation; and are aware of the consequences of non-compliance

Ensure confidential, personal or special category information is protected from view by unauthorised individuals

Keep passwords secret and do not allow anyone else to use your access to systems and accounts

Reporting any breach, or suspected breach of information security without delay

Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when leaving the office. Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Council property

Staff working from home must ensure appropriate security is in place to protect Council equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring Council equipment and information is kept out of sight. Council issued equipment must not be used by non-Council staff.

Use of personal devices to access Council systems is not permitted

Regularly conducting internal and external penetration tests and ensuring that outcomes are acted

Monitoring

The Council maintains the right to examine any system or device used in the course of our business, and to inspect any data held there.

To ensure compliance with this policy, the volume of internet and network traffic, and the use and content of emails and visited internet sites, may be monitored. Specific content will not be monitored unless there is suspicion of improper use.

It is the employee's responsibility to report suspected breaches of security policy without delay to their line manager.

All breaches of this policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the Council's disciplinary procedures.

Policy review

The policy will be reviewed on an annual basis and updated as necessary at these reviews.