## ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

# SECURITY POLICY

# SECURITY INCIDENT REPORTING

### Introduction

The council handles a large amount of financial, personal and sensitive information, including information about members of the public. This information is protected, but sometimes things go wrong and a security incident may occur.

### What is a Security Incident?

A security incident is defined as, ‘any event that may threaten or cause a security breach’. An incident report must be submitted after a security breach, and may be submitted if there is a concern about the possibility of a future security breach.

### Policy Statement

The council is responsible for the protection of its employees, buildings, information assets, IT systems and other facilities. It requires that actual or suspected security incidents are reported. Incidents will be prioritised, investigated and action taken to minimise any actual, or potential, risk to the public and the council.

Anyone working for the council must report a security concern, or an actual security breach, as soon as possible after it is discovered or anticipated.

The council will forward details of IT security incidents that need escalation to Government and other agencies, e.g. GovCertUK, Public Services Network authority.

### Not Covered by this Policy

If the council employs a partner organisation to provide services, it is possible that security incident reporting and management may become the responsibility of the partner. This must be agreed in the contract with them or in related agreements.
In this case the partner’s security incident reporting/management policy will apply.

### Those Affected by the Policy

This policy applies to any person performing duties on the council’s behalf in any location. For example, all users of the council's office and computer facilities including external third parties; council employees and workers, or Councillors who use their own IT equipment when working on council business.

### Roles and Responsibilities

1. Council employees, others working for the council, and users of council facilities – must report security incidents or concerns as soon as possible.
2. External service providers – must report security incidents or concerns to the appropriate council manager as soon as possible.
3. Council Heads of Service, Service Leads, Managers and Team Leaders – must ensure staff formally report incidents. They must take agreed action(s) to reduce the risk of incident repetition.
4. Information Governance Team – must manage and prioritise RBWM security incidents or oversee their resolution by partner organisations. The team must also ensure that incidents and any improvements made are communicated to council staff.

5. The Council's Data Protection Officer – must assess the impact of personal data loss or disclosure, and advise on whether a breach disclosure report to the Information Commissioner is required. If so, must complete the ICO's reporting form and communicate the ICO's feedback.
6. Audit & Investigations Service – may oversee the investigation of theft or fraud.
7. The IT Service - must investigate, manage and resolve the IT aspects of all incidents.
8. The Facilities Service – must investigate and advise on the physical security aspects of incidents. Also, assist in liaison with the police and provide support for police investigations.
9. Head of IT Service – responsible for forwarding details of IT security incidents that need escalation to Government and other agencies, e.g. GovCertUK, Public Services Network authority.

## Applying the Policy

Incidents may be reported in several ways. The preferred method is by using the electronic security incident reporting form on the council's Intranet site. They may also be reported by telephone or verbally to the council manager responsible, who must then submit an incident report. An incident may also be reported by emailing security@rbwm.gov.uk or the Customer Contact Centre.

When a security incident report form is submitted, an incident number will be issued and details of the incident report returned to the person submitting the form.
The details are also forwarded to the:

1) manager responsible for council facilities and the Facilities Team Leader
2) nominated Director, Head of Service or council manager
3) Information Governance Team
4) Council's Data Protection Officer
5) Other appropriate specialists and council officers.

## Policy Compliance

Compliance with this policy reduces the risk of damage to individuals and the council. Benefits include better protection for the public, reduced exposure of the council to legal action, financial loss, embarrassment, or disruption.

Any non-compliance with this policy could constitute a disciplinary offence. If you do not understand the policy, or how it applies to you, seek advice from the council manager responsible for your work, or from the Information Governance Team.

## Related Legal and Regulatory Obligations

UK Data Protection Act Information Security Standard ISO/IEC 27001:2005