www.rbwm.gov.uk

Royal Borough
of Windsor &
Maidenhead

Royal Borough Windsor & Maidenhead

Reporting Security Incidents Policy

June 2020

“Building a borough for everyone – where residents and businesses grow, with opportunities for all”

Our vision is underpinned by six priorities:

Healthy, skilled and independent residents
Growing economy, affordable housing
Safe and vibrant communities
Attractive and well-connected borough
An excellent customer experience
Well-managed resources delivering value for money

CONTENTS

Frequently used acronyms

IT	Information Technology
RBWM	Royal Borough of Windsor & Maidenhead
ICO	Information Commissioner’s Office

1 PURPOSE

1.1 The Royal Borough of Windsor and Maidenhead council processes a large amount of financial, personal, and sensitive information to operate and carry out our functions. These may include data from members of the public, current, past, and prospective employees and Councillors, clients, customers, suppliers, and partner organisations. In addition, RBMW may be required to process personal data to comply with the requirements of central government and law agencies.

1.2 The Royal Borough of Windsor and Maidenhead (RBWM) takes its obligations regarding compliance with the UK Data Protection Act 2018 (DPA 2018) and the EU General Data Protection Regulation (GDPR) very seriously.

1.3 The council has a duty under the DPA 2018 and the GDPR to ensure that the personal data it processes is kept safely and securely. This information is protected, but if a security incident may occur this **Security Incident Reporting Policy** should ensure that the applicable and relevant security controls are set in place in line with the Royal Borough of Windsor and Maidenhead requirements.

1.4 This policy puts into place a procedure for recording security incidents and dealing with any breaches of personal data which may occur, focussing on the steps to be taken once a breach has been discovered, and the processes all staff, including contractors and vendors with access to the Royal Borough of Windsor and Maidenhead systems, should follow.

1.5 All security incidents must be managed in an efficient and time effective manner to make sure that the impact of an incident is contained and the consequences for the council are limited. This document sets out the plan for reporting and dealing with security incidents at Royal Borough of Windsor and Maidenhead.

2 SCOPE

2.1 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.

2.2 The aim of this this policy is to prepare Royal Borough of Windsor and Maidenhead to ensure that the correct processes and procedures, roles and responsibilities are in place and followed for any council cyber threat or incident while normal business operations continue. This policy will also minimise the risk of further disruption to services.

2.3 Security Incidents includes any incident that occurs by accident or deliberately that impacts communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services in the council. This includes unauthorised access to, use, disclosure, modification, or destruction of data or services used or provided by the council.

2.4 The Information Commissioner's Office (ICO) can impose significant fines on data controllers for serious breaches of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 where the security of personal data is concerned. Sanctions applied by the ICO can also lead to reputational damage for the organisation.

2.5 The ICO can also serve an enforcement notice on a data controller to bring about compliance. It is possible to receive a fine and an enforcement notice.

2.6 This policy aims to provide a consistent approach and follows guidance provided by the ICO. However, dealing with incidents of breaches of data is complex; there are many potential variables and a balanced judgement needs to be taken on a case by case basis.

2.7 The GDPR requires that serious personal data breaches be reported to the ICO within 72 hours, with the ICO having the ability to impose fines for non-reporting.

2.8 This guidance is to set out clear reporting methods for cyber security incidents to be reported to the National Cyber Security Centre (NCSC) and where appropriate, fraud and cyber-crime being reported to the National Crime Agency (NCA), through Action Fraud.

2.9 It is the responsibility of the council to develop an effective incident management process and response plan. The response plan and assignment of responsibilities will be covered in the **Security Incident Response Plan** which can be found on the council's web site.

3 APPLICABILITY

3.1 This policy applies to all council employees and RBWM Councillors. This policy also applies to contractors, temporary, agency staff, partners and others working in a similar capacity that can access, manage, or process information assets of the council. They are also accountable for understanding and adhering to the guidance contained in this policy and any applicable supporting policies and procedures. All applicable persons listed above are referred to as 'users' in this policy.

4 AUTHORISATION

4.1 The legal and compliance reporting requirements the council must meet are documented.

4.2 Only authorised persons should have access to council assets and systems or accessing the council IT or mobile network. Any user that deliberately or inadvertently accesses the council IT or mobile network or systems unauthorised, will be in breach of this policy.

4.3 For any council business:

- Users accessing council IT facilities must comply with all council policies and procedures.
- Managers and team leaders must ensure their staff comply with this policy and provide advice to them.
- Managers and team leaders must ensure security incidents are raised in response to IT access security concerns or personal data breaches as covered in this policy.
- IT services provide technical solutions to support different IT access security levels, depending on the sensitivity and value of the data accessed.
- IT services ensure that privileged and systems administrator access is strictly controlled for all applications they administer based upon a valid business justification and specific job requirements as approved by the user's line managers.

5 POLICY COMPLIANCE

5.1 Compliance Measurement

5.1.1. All users must comply with this policy.

5.1.2. IT Services will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1.3. If you do not understand the implications of this policy, how it may apply to you, or your security responsibilities when working with the council, please seek advice in advance from your line-manager or contact the council's Data Protection Officer at **dpo@rbwm.gov.uk**.

5.2 Exceptions

5.2.1. Any exception to the policy must be approved by the IT Senior Management Team in advance.

5.3 Non-Compliance

5.3.1. Any breach of this policy may be subject to disciplinary action under the council’s disciplinary procedures, up to and including dismissal. In circumstances where it is believed that a criminal offence has been committed the matter may be reported to the Police.

6 SECURITY INCIDENT

6.1 A security incident can be defined as any event which has caused or has the potential to cause damage to the council's information assets and will include, but is not limited to:

6.1.1. Unauthorised persons gaining or seeking to gain access to council premises or those of business partners.

6.1.2. Unauthorised persons gaining or seeking to gain access to the council's information systems, whether operated by, or on behalf of the council.

6.1.3. Loss, theft, misuse, damage or destruction of any council information asset or equipment.

6.1.4. Computer virus import or infection.

6.1.5. Loss or theft of hard copy documents containing personal information.

6.1.6. Unforeseen incidents such as flood or fire.

6.1.7. Hacking attacks.

6.1.8. Use of unauthorised usb devices or media in council machines.

6.1.9. Failure to make adequate arrangements for information backup.

6.1.10. Unauthorised copying, amendment or deletion of data or software.

6.1.11. Unauthorised copying or use of access security cards.

6.1.12. Unauthorised disclosure or use of passwords, data, or software.

6.1.13. Alteration, falsification or tampering with audit records or evidence.

6.1.14. Unauthorised monitoring of information systems, employees, or business partners.

6.1.15. Use of the internet in contravention of UK law and the council's Use of Internet Policy.

6.1.16. Any offence where information is obtained by deception.

6.1.17. Information being disclosed inappropriately, for example, to unintended recipients or published on a website.

6.1.18. 'Card Account Data Compromise' – this is a security incident specific to payment card data. It is any event that results in unauthorised access to or exposure of payment card data (cardholder data or sensitive authentication data).

6.1.19. A data breach can be defined as the loss, disclosure, or inappropriate access to personal information as a result of a security incident.

6.1.20. Once a security incident has been discovered and reported, the data protection officer will determine whether a personal data breach has resulted from the incident.

6.1.21. Personal data losses not only effect of the individuals concerned, but also the efficiency of the service and the reputation of the council.

7 ROLES AND RESPONSIBILITIES

7.1 All council users must report a security incident, security concern, or an actual security breach, immediately after an incident or breach has been discovered or anticipated.

7.1.1. Council users, others working for the council, and users of council facilities must report security incidents or concerns as soon as they become aware of a potential incident.

7.1.2. External service providers must report security incidents or concerns to the appropriate council manager as soon as they become aware of a potential incident.

7.1.3. Heads of service, service leads, managers and team leaders must ensure staff formally report incidents. They must take action to reduce the risk of incident repetition.

7.1.4. IT services must manage and prioritise council security incidents or oversee their resolution by partner organisations. IT services must also ensure that incidents and any mitigation are communicated to council staff.

7.1.5. The Council’s data protection officer (DPO) must assess the impact of personal data loss or disclosure and determine whether the ICO and/or the data subject(s) affected by a personal data breach should be notified. It is the DPO’s responsibility to ensure that mitigating controls recommended by the ICO are implemented, if required and that any learning outcomes identified by the ICO in respect of the breach are communicated to the Senior Information Risk Officer (SIRO) and to the wider organisation.

7.1.6. Audit & investigations service may oversee the investigation of theft or fraud.

7.1.7. IT services must investigate, manage, and resolve the IT aspects of all incidents.

7.1.8. 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.

7.1.9. Head of HR, corporate projects and IT is responsible for forwarding details of IT security incidents that need escalation to Government and other agencies, e.g. GovCertUK, Public Services Network authority.

7.2 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.

7.3 In this case the partner's security incident reporting/management policy will apply.

7.4 **All users must**:

7.4.1. Make sure they understand how to identify and report a suspected or actual security incident.

7.4.2. Report any security related issues or concerns, or an actual security incident to their manager or to a member of the **Security Incident Response Team** (SIRT).

7.5 **The Incident Response Lead is responsible for:**

7.5.1. Making sure that the **Security Incident Response Plan** and associated response and escalation procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.

7.5.2. Making sure that the security incident response plan is up to date, reviewed and tested, at least once each year.

7.5.3. Making sure that staff with security incident response plan responsibilities are properly trained, at least once each year.

7.5.4. Leading the investigation of a suspected breach or reported security incident and initiating the security incident response plan, as and when needed.

7.5.5. Reporting to and liaising with external parties, including the acquirer and card brands, legal representation, law enforcement, etc. as is required.

7.5.6. Authorising on-site investigations by appropriate law enforcement or payment card industry security/forensic personnel, as required during any security incident investigation. This includes authorising access to/removal of evidence from site.

7.6 **Security Incident Response Team (SIRT) are responsible for:**

7.6.1. Making sure that all council users understand how to identify and report a suspected or actual security incident.

7.6.2. Advising the incident response lead of an incident when they receive a security incident report from council users.

7.6.3. Investigating each reported incident.

7.6.4. Taking action to limit the exposure of sensitive or payment card data and to reduce the risks that may be associated with any incident.

7.6.5. Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls.

7.6.6. Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.

7.6.7. Reporting each security incident and findings to the appropriate parties. This may include the acquirer, card brands, third party service providers, business partners, customers, etc., as required.

7.6.8. Assisting law enforcement and card industry security personnel during the investigation processes. This includes any forensic investigations and prosecutions.

7.6.9. Resolving each incident to the satisfaction of all parties involved, including external parties.

7.6.10. Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.

7.6.11. Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

8 INCIDENT REPORTING

8.1 As soon as an incident has been identified, the user concerned must report the incident immediately.

8.2 Incidents can be reported in several ways. The preferred method is by using the **Report an IT / Security Concern/Incident or Report a Data Protection Concern/Incident** forms 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 services contact centre. Where the incident involves personal data, the DPO may also be contacted directly at DPO@rbwm.gov.uk.

8.3 When an incident reporting form is submitted, an incident number will be issued, and details of the incident report returned to the person submitting the form.

8.4 The details are also forwarded to the:

8.4.1. manager responsible for council facilities and the Facilities Team Leader.

8.4.2. nominated Director, Head of Service or council manager.

8.4.3. Council's Data Protection Officer.

8.4.4. Other appropriate specialists and council officers.

8.5 It is recommended that a senior officer from the service area is nominated as ‘incident owner’ and that the relevant Head of Service is informed.

8.6 If an incident is suspected to have taken place the following information will be required to assess the seriousness of the breach:

8.6.1. The type of data involved.

8.6.2. How sensitive the data is? Is it personal data?

8.6.3. If the data has been lost or stolen, whether there are any protections in place e.g. encryption.

8.6.4. What has happened to the data?

8.6.5. What could the data tell a third party about an individual?

8.6.6. The volume of data i.e. how many individuals’ personal data are affected by the breach.

8.6.7. Who are the individuals whose data has been breached?

8.6.8. What harm can come to those individuals?

8.6.9. Are there wider consequences to consider e.g. loss of public confidence, negative publicity, financial implications?

8.7 If after the initial assessment a personal data breach has been clearly identified, then an incident response team should be co-ordinated by the data protection officer. This should include the key officers involved in the breach. Depending on the nature of the incident, it may be necessary to alert the council’s corporate communications team to prepare if required to deal with any media enquiries.

8.8 The key officers involved should be proportionate to the type of incident. For instance, a minor personal data breach may require involvement of the following officers:

8.8.1. Line manager.

8.8.2. Senior officer (breach owner).

8.8.3. Data protection officer.

8.8.4. Head of HR, Corporate Projects and IT (for incident is IT related).

8.8.5. Head of service.

8.9 A serious breach, whether in terms of size of breach, or sensitivity of information, may require involvement of the following officers:

8.9.1. Managing Director

8.9.2. Senior Information Risk Officer

8.9.3. Executive Director

8.9.4. Head of Service

8.9.5. Legal services manager

8.9.6. Senior officer (Incident Response Lead)

8.9.7. Data Protection Officer

8.9.8. Head of HR, Corporate projects and IT.

8.9.9. Audit manager

8.9.10. Customer services manager

8.9.11. Communications and marketing manager

8.10 The head of service, or their nominated deputy, should liaise with the data protection officer to consider the action to be taken to:

8.10.1. Protect the interests of the customer.

8.10.2. Ensure the continuing delivery of the service.

8.10.3. Protect the interests of the council.

8.10.4. Meet the requirements of the GDPR in terms of informing the ICO.

8.11 Incidents will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary:

8.11.1. damage limitation.

8.11.2. establishing who needs to be made aware of the incident and informing them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment, or simply changing access codes.

8.11.3. establishing whether losses can be recovered, and damage can be limited.

8.11.4. fully assessing the risk in terms of the potential adverse consequences for individuals. How serious or substantial are the consequences, how likely are they to happen and what needs to be put in place to provide protection to those affected by the incident.

Testing and updates

8.12 Annual testing of the incident response plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the security incident response team are aware of their obligations, unless real incidents occur which test the full functionality of the process.

8.12.1. The incident response plan will be tested at least once annually.

8.12.2. Testing responses to different potential incident scenarios to identify process gaps and improvement areas in the incident response plan.

8.12.3. The security incident response team will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.

8.12.4. The incident response lead will ensure the security incident response plan is updated and distributed to security incident response team members.

9 INCIDENT RESPONSE PLAN STEPS

The following steps must be followed with all security incidents

9.1 Report

9.1.1. Information security incidents must be reported, without delay, to the incident response lead (preferable) or to another member of the security incident response team. The member of the security incident response team receiving the report will advise the incident response lead of the incident.

9.1.2. In the event that a security incident or data breach is suspected to have occurred, we recommend the staff member discuss their concerns with their line manager, who in turn may raise the issue with a member of the security incident response team.

9.2 Investigate

9.2.1. After being notified of a security incident, the security incident response team will perform an initial investigation and determine threat level and the appropriate response, which may be to initiate the council's security incident response plan.

9.2.2. If the security incident response plan is initiated, the security incident response team will investigate the incident and initiate actions to limit the exposure of cardholder data and in mitigating the risks associated with the incident.

9.2.3. Initial incident containment and response actions are:

- Make sure that no-one can access or alter compromised systems.
- Isolate compromised systems from your network and unplug any network cables – without turning the systems off.
- If using a wireless network, change the SSID (Service Set Identifier) on the wireless access point and other systems that may be using this wireless network (but not on any of the systems believed to be compromised).
- Preserve all logs and similar electronic evidence, e.g. logs from your firewall, anti-virus tool, access control system, web server, application server, database, etc.
- Perform a back-up of your systems to preserve their current state – this will also facilitate any subsequent investigations.

- Keep a record of all actions you and all members of the Security Incident Response Team take.
- Stay alert for further indications of compromise or suspicious activity in your environment, or that of your third parties.
- Seek advice before you process any further payment card transactions.
- If you can, gather details of all compromised or potentially compromised payment card numbers (the ‘accounts at risk’).

9.3 Inform

9.3.1. Once the security incident response team has completed their initial investigation of the security incident:

- The incident response lead will inform Head of HR, corporate projects and IT.

9.3.2. The incident response lead and / or the security incident response team member responsible for communications will inform all relevant parties. This includes your acquirer and local law enforcement, and other parties that may be affected by the compromise such as your customers, business partners or suppliers. This also includes the personal data breach notification contacts, as applicable to the incident under investigation.

9.4 Business continuity

9.4.1. The security incident response team will engage with operational teams in your services to make sure that your service can continue to operate while the security incident is being investigated.

9.4.2. Plan for any security incident that may impact on council business to ensure business continuity:

- Make sure you have system and data backups available in the event of loss of data, system corruption/virus infection or hardware failure.
- Consider what offline or alternative payment acceptance methods to use if the council were unable to take card payments on the ConnectPay portal website.

9.5 Resolve

9.5.1. The members of the security incident response team will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation that the required controls and security measures are operational.

9.5.2. The incident response lead will report the investigation findings and resolution of the security incident to the appropriate parties and stakeholders.

9.6 **Recovery**

9.6.1. The incident response lead will authorise a return to normal operations once satisfactory resolution is confirmed.

9.6.2. The security incident response team will notify the rest of the business that normal business operations can resume. Normal operations must adopt any updated processes, technologies or security measures identified and implemented during incident resolution.

9.7 **Review**

9.7.1. The security incident response team will complete a post-incident review after every security incident. The review will consider how the incident occurred, what the root causes were and evaluate the effectiveness of the response.

9.7.2. For all security incidents where systems, policies or allocation of responsibilities was found to be at fault, carrying on 'business as usual' may not be acceptable. Improvements should be instigated as soon as possible and should be communicated to managers and staff and recorded so the council can be seen to have reacted in a responsible manner.

9.7.3. Those investigations into the cause of the loss of data should consider the lack of staff competence or training and where appropriate, action may be considered under the council's disciplinary procedure,

9.7.4. If the breach was caused, even in part, by systemic and ongoing problems, then action will need to be taken and procedures in place to prevent any recurrence in the future. This will help to identify recommendations for better future responses and to avoid a similar incident in the future.

9.7.5. Changes and updates that may be required include:

- Updates to the security incident response plan and associated procedures.
- Updates to the council's security or operational policies and procedures.
- Updates to technologies, security measures or controls.
- The introduction of additional safeguards in the environment where the incident occurred (for example, more effective malware protection).
- The security incident response team will ensure that the required updates and changes are adopted or implemented, as necessary.

Document Name	**Reporting security incidents policy**		
Document Author	**Infrastructure security manager**		
Document owner	**Head of HR, corporate projects and IT Services**		
Accessibility			
File location			
Destruction date			
How this document was created	Version 1	**18/07/2011**	**Security manager**
	Version 2	**19/10/2017**	**Security manager**
	Version 3	**25/06/2020**	**Infrastructure security manager**
Circulation restrictions			
Review date	**25/06/2022**		