Royal Borough Windsor & Maidenhead

Secure Portal Access Agreement

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

1 INSTRUCTIONS

1.1 Before an external Supplier, Partner or Third Party may gain access to the RBWM Portal they must read the **RBWM Supplier and Third-Party IT Acceptable Usage Policy**.

1.2 They must then complete the **Secure Portal Access Agreement Form** in the Appendices section in this document.

1.3 There are three sections to complete.

1.3.1. **SECTION 1** – To be completed by the RBWM manager.

- Authorises portal access and defines personnel security checks if needed.
- The RBWM manager then sends the User Agreement Forms and Portal Access Conditions to the external organisation's manager to complete Section 2 and 3.

1.3.2. **SECTION 2 & 3** – To be completed by the external organisation's manager.

- **SECTION 2A** – Provide all the technical information needed to set up the remote access.
- **SECTION 2B** – Include name, signature, email, and date for every person who requires access from the external organisation. This section provides a signed declaration by everyone who is applying for access promising to comply with the RBWM Supplier and Third-Party IT Acceptable Usage Policy.
- **SECTION 3** – Confirms security check results (if required). It contains the external manager's signed commitment to comply with the Council's security requirements.

1.4 RETURN OF FORMS

1.4.1. The External Manager must return the forms to the RBWM IT Security Manager (**security@rbwm.gov.uk**).

1.4.2. The form will be checked and authorised before external portal access will be set up for the named persons.

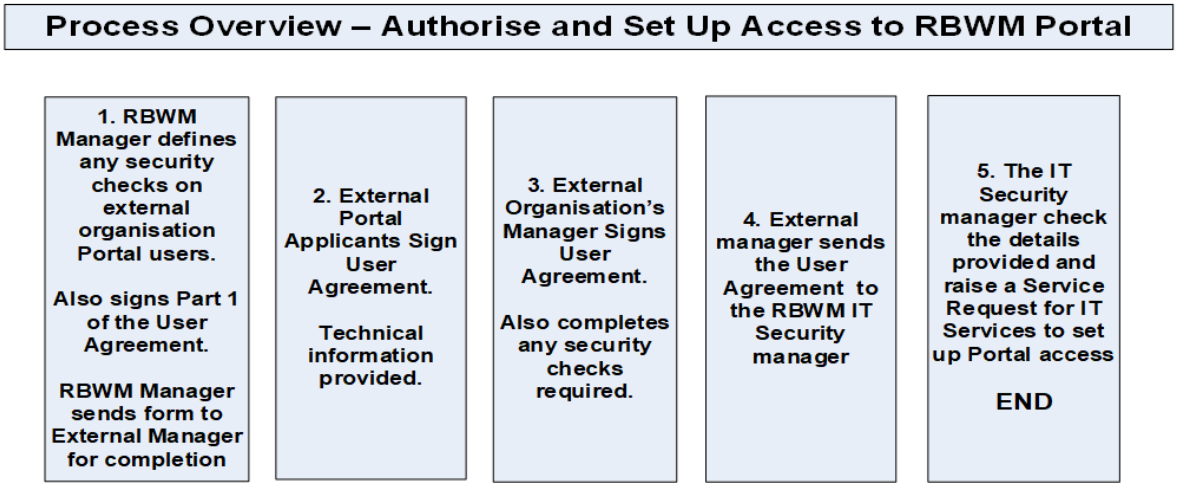
2 PURPOSE

2.1 This document outlines the access conditions governing remote access to the Royal Borough of Windsor & Maidenhead's (RBWM's) Internet Portal by external organisations.

2.2 All applicants to use the RBWM Portal who are not direct employees of RBWM must sign Section 2B of the User Agreement Form (Appendix A).

2.3 These applicant's manager must sign Section 2A and Section 3 of the User Agreement Form (Appendix A).

2.4 The five-step set-up process is shown below.



3 DEFINITIONS

3.1 The "Portal" is defined as either a secure website that offers a variety of online services, or remote access Virtual Private Network (VPN) connections such as Site 2 Site (Fixed) or dial on demand VPN Connections (Flexible).

3.2 The RBWM Portal provides password and other security protection, and then permit access to a personalised set of software, Internet, and file access services.

3.3 A "Supplier", "Partner" or "Third Party" is an organisation and its employee(s) who apply to access the Council's IT facilities and information through the RBWM Internet Portal. This access can be for a variety of reasons including IT support, collaborative working between RBWM and other organisations, or for commissioned work for the Council.

3.4 The Secure Portal Access Agreement is a signed agreement to comply with the Council's security policies and procedures when using the Portal.

3.5 Exceptions

Any exception to the policy must be approved by the IT Senior Management Team

4 APPLICABILITY

4.1 All partners, suppliers and third parties requiring access to the Council's IT facilities using the RBWM Internet Portal must read this document before completing and signing the Portal User Agreement.

4.2 The Secure Portal Access Agreement form must be returned with the signature of everyone who will use the Portal and the supporting signature of:

4.2.1. The RBWM manager responsible for the access request, and

4.2.2. The signature of either:

- a senior company representative, e.g. Director; for commercial companies; or
- a senior manager for not-for-profit or public sector organisations.

5 AUTHORISATION

5.1 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.

5.2 For any council business:

5.2.1. Users accessing council IT facilities must comply with all council policies and procedures.

5.2.2. Managers and Team Leaders must ensure their staff comply with this policy and provide advice to them.

5.2.3. Managers and Team Leaders must ensure security incidents are raised in response to IT access security concerns or security breaches as covered in the **Reporting Security Incidents Policy**.

5.2.4. IT Services provide technical solutions to support different IT access security levels, depending on the sensitivity and value of the data accessed. Administer, control, and monitor access to IT facilities and systems.

5.2.5. IT Services ensure that privileged and systems administrator access is strictly controlled based upon a valid business justification and specific job requirements as approved by the user's line managers.

6 POLICY COMPLIANCE

6.1 Compliance Measurement

6.1.1. All partners, suppliers and third parties accessing to the Council's IT facilities must comply with this form.

6.1.2. The Use of the Portal is monitored and may be audited from time to time.

6.1.3. User identifiers will be unique, must be kept secure, and can be used to trace any activity.

6.1.4. The IT Support 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.

6.1.5. 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**.

6.2 Non-Compliance

6.2.1. 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.

7 LEGAL REQUIREMENTS

The Council has a legal obligation to comply with the following laws and directives. They apply to all use of the RBWM Internet Portal.

7.1 The Computer Misuse Act 1990

This includes the following computer related offences:

7.1.1. The unauthorised access to RBWM systems and data.

7.1.2. The unauthorised access with intent to commit or facilitate the commission of further offences (such as fraud or theft)

7.2 **The Data Protection Act 2018**

7.2.1. All personal and sensitive personal data held on RBWM systems is processed in compliance with the eight principles of the Data Protection Act 2018.

7.2.2. The main principle that applies to use of the Portal is the sixth data protection principle:

- Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.
- The risks referred to in subsection (1) include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification, or disclosure of, personal data.

7.3 **The Freedom of Information Act 2000**

7.3.1. Information held by RBWM may be disclosed in response to requests made under the general right of access.

7.3.2. The Privacy and Electronic Communications (EC Directive) Regulations 2003

7.3.3. This Directive expressly addresses network security and the security of electronic communications services, and places RBWM under an obligation to take appropriate technical and organisational measures to safeguard the security of the service (network).

7.4 **Human Rights Act 1998**

7.4.1. All information and data are processed under the Convention Rights of the Act.

8 CONDITIONS OF USE

8.1 All users of the Council's IT facilities must agree to comply with all of the conditions of use in the **Supplier and Third-Party IT Acceptable Usage Policy.**

8.2 Two important conditions of use address IT access security risks:

8.2.1. You will keep your user identifier and password secret.

8.2.2. Under no circumstances will you share your user identifier or password with someone else, or sign onto systems on their behalf.

8.3 Failure to comply with any of the conditions in the Supplier and Third-Party IT Acceptable Usage Policy will be regarded as a serious breach of the Council's security policies and will result in Portal access being revoked.

9 SECURITY CLEARANCE

9.1 The RBWM manager who authorises external access through the Internet Portal is responsible for defining the level of security clearance required.

9.2 Access to personal and sensitive data will normally require a current DBS or Basic Criminal Record Disclosure certificate, e.g. for Social Services; Revenues & Benefits; Human Resources.

9.3 It is the external manager's responsibility to ensure that all security checks requested by RBWM are completed and evidence provided. Access will not be permitted without the required security clearance.

10 PORTAL ACCESS PROCEDURES

10.1 The RBWM manager must complete section 1 of the User Agreement and then send it to the external organisation, who must complete and sign sections 2 and 3.

10.2 The forms must then be returned to the RBWM IT Security manager (**security@rbwm.gov.uk**) who will check and action the request.

11 TECHNICAL SET-UP AND SECURITY

11.1 Several types of Partner portal security can be provided:

11.1.1. **Digitally Certificated Security**

- This combines a user identifier and session password check with a digital certificate check by an RBWM server computer.

11.1.2. **Authentication Token Security**

- In addition to a user identifier and session password, the portal user must use a physical authentication token to obtain an additional access security code.

11.1.3. **Site to Site VPN**

- A fixed site to Site VPN Tunnel between the RBWM network and the third-party network. Normally used for development work, or where the Partner Portal is not suitable.

12 TERMINATION OF PORTAL ACCESS RIGHTS

12.1 RBWM IT Services will be notified immediately in the event of any authorised Portal user terminating employment, having a change in job role, or if there are security concerns about an individual.

12.2 Portal access must be reviewed as soon as IT Services were notified about any role change or concern and disabled if necessary.

12.3 Portal access must be disabled immediately if a security breach is possible. Portal access must be reviewed annually and disabled if no longer required.

13 PORTAL SUPPORT

13.1 RBWM IT Services must be contacted if support is required or problems arise when using RBWM Portals. Examples include being unable to Login; being unable to use the authentication token; or not being able to access applications on the Portal.

Contact Information

Information Technology Services
Royal Borough of Windsor and Maidenhead
Town Hall, St. Ives Road, Maidenhead SL6 1RF
Tel. 01628 683800.

RELATED STANDARDS, POLICIES AND PROCEDURES

- Supplier and Third-Party IT Acceptable Usage Policy
- Reporting security incidents policy.
- The Computer Misuse Act 1990.
- UK Data Protection Act 2018.
- Human Rights Act 1998.
- The Freedom of Information Act 2000.
- Information Security Management Standard ISO/IEC 27001:2013.
- NIST SP800-63.3 standards

Document Name	**Secure Portal Access Agreement**		
Document Author	**Peter Strode**		
Document owner	**Nikki Craig**		
Accessibility			
File location			
Destruction date			
How this document was created	Version 1	**18/10/2010**	**Peter Strode**
	Version 2	**23/10/2014**	**Peter Strode**
	Version 3	**25/06/2020**	**Simon Arthur**
Circulation restrictions			
Review date	**25/06/2021**		

APPENDICES

Royal Borough Windsor & Maidenhead

Secure Portal Access Agreement Form

SECTION 1

(completed by the RBWM Manager)

1.1 Organisation Requiring Secure Portal Access

1.2 Summary of Systems and Data plus Business Reason for Access

1.3 Security Clearance

Is security clearance required (select one)? **YES / NO**

What Personnel Security Clearance is required?

Type of Security Clearance	Required (Yes/No)?
Basic DBS Check	
Enhanced DBS Check	
Basic Criminal Record Disclosure Check	
Other type of check	

Provide details of any other type of check below.

1.4 RBWM Manager's Confirmation

I authorise portal access for the named organisation on condition that access requirements are provided and accepted by RBWM IT Services. Also, on condition that any required security checks are completed.

I accept responsibility for ensuring that external users understand and comply with the RBWM procedures and conditions, and also the **RBWM Supplier and Third-Party IT Acceptable Usage Policy**.

Print Name of RBWM Manager	**Signature**

Job Title or Position	**Date**

Contact Telephone Number	**Email Address**

SECTION 2A

(to be completed by the external organisation's manager).

2.1 Organisation Requesting Secure Portal Access

2.2 Portal Access Requirements

Systems Access	Data Access

2.3 When will access be required?

Is permanent access required? **YES / NO** (please select)

2.4 What operating system will you use to access the Portal?

2.5 What Internet browser do you use to access the Portal?

2.6 User Details and Signature

This information has been provided by the following:

Print Name	Signature

Job Title or Position	Date

Contact Telephone Number	Email Address

SECTION 2B

(to be signed and dated by every person who requires access through the Secure Portal)

2.7 Organisation Requesting Secure Portal Access

2.8 Portal User Agreement and Signatures

I agree to the procedures and conditions in the **RBWM Supplier and Third-Party IT Acceptable Usage Policy** at all times. I will also comply with any related policies and procedures that I may need to use when providing services to the council.
I understand that failure to comply with the above policy will lead to action by the council.
I will comply with any IT (or information access) rights granted by the Royal Borough of Windsor and Maidenhead, and ensure I understand the business reasons for these rights.
I also understand that my breach of any access rights I am granted to access either council information or IT facilities, will lead to action by the council.
I also have any required security clearance.

Please sign and date in the boxes below.

Print Name	Date	Signature	Email Address

SECTION 3

(to be completed by the external organisation's manager).

3.1 Organisation Requesting Secure Portal Access

3.2 Personnel Security Clearance

Please provide any required security clearance evidence below.

NOTE The external manager must sign and date Section 3 overleaf to confirm request completion and commitment to the Council's security requirements.

Person's Name	Clearance Type and Number	Date Clearance Awarded

3.3 External Manager's Authorisation

I confirm that the information provided is accurate and that where requested, the required security checks have been completed and details confirmed.

I also agree to the procedures and conditions in the RBWM Portal Access Conditions and to those in the **RBWM Supplier and Third-Party IT Acceptable Usage Policy**.

Print Name of External Manager/Authoriser	**Signature**

Job Title or Position	**Date**

Contact Telephone Number	**Email Address**

PLEASE RETURN ALL FORMS TO THE IT SECURITY MANAGER

Contact Information:

IT and Change Service,
Corporate Services Directorate
Royal Borough of Windsor and Maidenhead
Town Hall,
St. Ives Road,
Maidenhead
SL6 1RF