Security Policy
Supplier and Third Party IT Acceptable Usage Policy

1 Introduction
This policy defines the security conditions for external suppliers, contractual third parties and agents, external organisations and others who provide services to the council using IT facilities. The IT facilities they use may either be council IT facilities or their own. All of the above are required to read the policy, and confirm agreement in writing.

2 Policy Statement
The Royal Borough of Windsor and Maidenhead requires all external service providers to understand and comply with the council's security conditions, including where necessary those agreed with central government as part of Government Connect.

3 Policy Aim and Benefits
The council recognises the risks associated the use of IT facilities and when handling council information when conducting council business. The policy aims to reduce risks arising from: (a) unauthorised access to buildings, IT equipment or systems; (b) loss, theft or misuse of information; (c) misuse of IT systems; and (d) legal non-compliance

4 Not covered by this Policy
Additional security requirements contained in the supplier's or external organisation's own Information Security policies and procedures.

5 Acceptable Usage Conditions
All those providing council services by either utilising council IT facilities or their own IT facilities must be aware of, and comply with, the security conditions below. They are required to:

<u>Legal</u>

1. Accept that their use of council IT facilities may be monitored and/or recorded for lawful purposes;

2. Comply with the UK Data Protection Act and all other legal, statutory or contractual obligations;

<u>Access Control</u>

3. Never attempt to access council IT facilities without written permission, and only use authorised equipment at authorised locations;

4. Only access the council's IT facilities by using the user identifier and password provided by the council. Also ensure that their passwords are difficult to crack and changed regularly.

4b. Protect and never disclose council-issued user identifiers and passwords, and only use the user identifier(s) in an agreed manner;

5. Only access the council's IT facilities remotely by using a secure technology configuration and security framework as provided or defined by the council;

6. Never exchange data on portable media with the council, e.g. on USB memory sticks or DVD/CDs, without council authorisation. These media must be kept secure and locked away when not in use.

Further information is provided in the council's Storage of Information Policy.

6b. Always use the council's data exchange policies and procedures to provide security for once-off transfers of personal or sensitive data to or from the council;

Information and Data Handling Security

7. Always seek to prevent accidental disclosure of the council's sensitive or personal information, e.g. by the accidental overlooking or overhearing of such information;

8. To handle personal or sensitive council data, emails, or information with care, for example:
   - Use courier despatch for highly sensitive or personal data. It is recommended that this type of information be hand delivered, or delivered by a personal courier.
   - Do not leave printout containing personal or sensitive information unattended when printing
   - Hold telephone conversations in private areas, so that they cannot be overheard.
   - Keep personal or sensitive information or data locked away when not attended.
   - Dispose of this information by using a cross-cut shredder or a confidential waste service.

9. Protect and handle securely any electronic or paper council information when it is used, sent, received, stored or processed;

10. Never disclose any sensitive or personal council information unless satisfied that the recipient(s) have a 'need to know' and are authorised by the council to see it;

11. Never send files, web service data, or emails that contain sensitive or personal data across the public Internet without providing encryption protection.

Other Security Responsibilities

12. Ensure that any personnel security checks required by the council for individuals providing services to the council are completed and the results are checked and accepted before accessing the council's IT facilities or information.

    The council manager responsible for the service(s) provided must define the security checks required. This will ensure appropriate protection of the council's interests;

13. Take responsibility for secure use of council IT services and secure access to council information. This includes protecting and never disclosing user identifiers, passwords, access tokens, or any other access mechanisms;

Physical and Environmental Security

14. Return, or securely destroy in an agreed fashion, any council information or data used in the provision of services;

15. Take precautions to protect all computer media, portable computers, and electronic equipment (e.g. Internet phones) when carrying them in transit. For example, never leave a laptop, other equipment, or computer media, unattended;

Security Incident Reporting

16. Report all suspected or actual security breach to the council manager responsible, who can complete a Security Incident Report.

16b. Also inform the council's IT Service Desk as soon as possible to ensure that electronic equipment can be disabled if possible.

Protection Against Damage and Electronic Attack

17. Never knowingly cause any form of damage to the council's IT facilities, nor attempt to by-pass or subvert system security controls;

18. Never insert portable computer media into the council's IT network without first getting them checked for viruses and malware. This can be done by contacting the IT Service Desk. Further information is provided in the council's Receipt of External Data on Portable Computer Media Policy.

19. Ensure that any IT equipment used to provide services to the council is protected by anti-virus software and spyware, and that this software and any anti-virus definitions are always up to date. Also never knowingly introduce viruses or other malware into the council's IT network; nor knowingly disable anti-virus protection.

19b. Where a virus is suspected or detected, the matter must be reported to the council's IT Service Desk immediately. Until virus repair is effected, an infected computer must not be used. Virus repair must be undertaken only by (or under the guidance of) authorised IT support staff.

20. Never download software or programs (including screen savers and wallpaper) from the Internet or from removable media onto council IT equipment.
Software must only be installed onto council IT equipment by authorised staff.

21. Never disable any IT security safeguards that have been implemented on computer equipment used to provide the council with services;

Termination of Work

22. Before termination of the contract or work agreement, inform the council of any information held, and ensure that this information is either destroyed, stored under an agreement, or formally returned to the council.

23. Notify the council immediately if a provider of services to the council terminates their employment, or changes job, and their access to council IT facilities is no longer required.

Control of Changes

24. Ensure that all changes made to the council's IT programs, databases or files are authorised and documented and approved within the council's IT Change Control process.

6 Policy Compliance

The supplier or external organisation agrees to comply with the council's Conditions of Use described in Section 5. This policy must be adhered to at all times.

On written request from the council, details of steps taken to comply with this policy must be provided. This may be in addition to any other security checks and audits.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the council manager responsible, the IT Service, or the council's Information Governance team.

7 Related Policies and Information

Secure Data Transfer Policy and Data Transfer Agreement
Storage of Information Policy
Receipt of External Data on Portable Computer Media
Security Incident Reporting Policy