INFORMATION SECURITY POLICY

This policy provides internal guidance relating to the security of information and data held by the Council, whether that be in digital or hard copy, and the use of Council devices and information technology (IT) systems.

The obligations outlined in this policy apply to everyone who has access to, holds copies of or processes Council information. This includes staff members, meaning employees, agency staff and those retained on a temporary or permanent basis, and Councillors.

Separately, the Council's 'Data Protection Policy' provides specific guidance on the handling and processing of personal data held by the Council.

Introduction

Woodley Town Council handles information daily, including data which is considered sensitive. Sensitive information within this policy refers to any information or data which may be deemed to be confidential or personal data in line with the Council's Data Protection Policy.

Data may be handled and stored in hard copy format, such as written or printed materials, or in digital format on the Council's IT systems, such as on computers and other devices.

Details of the Council's IT infrastructure are provided as part of this policy, in **Appendix A**.

Information Security

Sensitive information must have adequate safeguards in place to protect personal data and privacy, and to ensure compliance with various regulations.

The Town Council commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end, the Council is committed to maintaining a secure environment in which to process information so that we can meet these promises.

Individuals handling sensitive information should ensure that they:

- Handle information in line with relevant Council policies, including the Data Protection Policy;
- Limit personal use of Woodley Town Council information and telecommunication systems;
- Do not use e-mail, internet and other Council resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware unless you have explicit management approval;
- Always leave desks clear of sensitive information and lock computer screens when unattended;
- Report information security incidents, without delay, to the Town Clerk or Deputy Town Clerk.

The Town Council reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.

We each have a responsibility for ensuring the Council's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from the Town Clerk or Deputy Town Clerk.

Acceptable Use

The Council is committed to protecting individuals and the Council itself from illegal or damaging actions, either knowingly or unknowingly by individuals.

- Individuals are responsible for exercising good judgment regarding the reasonableness of personal use.
- Individuals should take all necessary steps to prevent unauthorised access to sensitive information.
- Passwords must be kept secure and individual accounts must not be shared; authorised users are responsible for the security of their passwords and accounts.
- All devices (including Macs, PCs, laptops etc) should be secured with a password-protected screensaver to prevent unauthorised access.
- All devices should be appropriately protected and secured so they cannot be tampered with or altered.
- Where suspicious behaviour is identified it should be reported to the Town Clerk or Deputy Town Clerk as soon as possible.
- Portable devices (including laptops) are especially vulnerable and must be appropriately secured when not in use.
- Individuals must use extreme caution when opening e-mail attachments received from unknown senders which may contain dangerous or malicious content, such as viruses or malware.

Protect Stored Data

All sensitive information stored and handled by the Council and its individuals must be securely protected against unauthorised use at all times.

Where practical, hard copies of personal data received will be scanned and kept on the Council's IT servers, with hard copies treated as confidential waste and disposed of securely.

Any sensitive information that is no longer required for business reasons must be discarded in a secure and irrecoverable manner.

User Access Management

- Access to Woodley Town Council systems is controlled through a formal process, instigated following the hire of an employee / election of a Councillor.
- There is a standard level of access to Council information and data; access to certain sensitive information may be restricted unless the user is specifically authorised by the Town Clerk / Deputy Town Clerk or an appropriate manager.
- The job function of the user decides the level of access the employee has to sensitive information.
- Where absolutely necessary, and with the prior agreement of their Manager, individuals may access, create and store Council work on a personal device; this includes undertaking the filming / photography of Council events. Where this takes place, access to the personal device must be password protected, and any work must be transferred to a Council owned device as soon as possible and then deleted from the personal device.
- As soon as an individual leaves Woodley Town Council employment, all system logons must be immediately revoked.

Access to the Sensitive Information

All access to sensitive information should be controlled and authorised.

- No individuals shall have access to sensitive information unless they have a genuine business need.
- Sensitive information shall not be shared with any individual or organisation where there is no legitimate business reason to do so.
- Where sensitive information is legitimately shared outside of the Council (e.g. with a 3rd party service provider) the Council will ensure a written agreement is in place that the service provider will be responsible for any sensitive information the service provider possesses.
- Woodley Town Council will ensure that a there is an established process, including proper due diligence is in place, before engaging with a service provider.

Physical Security

Access to sensitive information held in either digital or hard copy format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Sensitive information must be handled and distributed in a secure manner.
- Email communication between individuals with Town Council email accounts (@woodley.gov.uk) should take place via the Council's email system, and not via personal email accounts. Related emails should not be sent or forwarded to an alternative, personal email address where any data included is, or might contain confidential or personal data.
- Visitors should be escorted by a trusted employee when in areas that hold sensitive information.
- All visitors that enter the Council's office area and / or server and archive room must sign in and wear a 'Visitors' badge for the duration of their visit, to enable staff to identify visitors in areas where sensitive information may be accessible. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the Council's offices who is not a Council employee or Councillor.
- Where access is granted to any third party personnel claiming to repair, maintain, install or replace devices or equipment, appropriate steps will be taken to verify their identity.

Disposal of Stored Data

- All sensitive information must be securely disposed of when no longer required by the Council, regardless of the method by or device on which it is stored, and whether it is stored in hard or digital format.
- The Council requires that hard copy materials are destroyed either by crosscut shredding, incineration or pulping, so they cannot be reconstructed; any hard copy materials awaiting destruction must be held in clear marked containers (e.g. marked "To Be Shredded"), access to which must be restricted
- When destroying digital copy materials, the Council requires that data must be rendered unrecoverable when deleted.

MANAGEMENT AND PROCESSING OF PAYMENT CARDHOLDER DATA

Access to Sensitive Cardholder Data

Access to sensitive cardholder data should be controlled and authorised.

- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to individuals that have a legitimate need to view such information.
- No other individuals should have access to this confidential data unless they have a genuine business need.

- Cardholder data will only be shared with a 3rd party service provider where the Council has entered into a formal Service Level Agreement with the provider.
- All third-party companies which have access to cardholder information must
  1. Adhere to the PCI DSS security requirements.
  2. Acknowledge their responsibility for securing the cardholder data.
  3. Acknowledge that the cardholder data must only be used for assisting the completion of a transaction, providing a fraud control service or for uses specifically required by law.
  4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
  5. Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.
- Woodley Town Council will have a process in place to monitor the PCI DSS compliance status of the Service provider.

Physical Security
It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance.

Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.

Credit Card (PCI) Security Incident Response Plan
Woodley Town Council's PCI security incident response plan is as follows:

1. Where an individual reasonably believes there may be a breach of cardholder information or of systems related to the PCI environment in general, they must report the incident to the Town Clerk or Deputy Town Clerk as soon as possible.
2. The Town Clerk / Deputy Town Clerk will investigate the incident and limit the exposure of cardholder data and in mitigating the risks associated with the incident.
3. The Town Clerk / Deputy Town Clerk will seek to resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
4. The Town Clerk / Deputy Town Clerk will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required.

In dealing with an incident, the Town Council will make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required, and assist in the investigative processes, including in prosecutions.

Credit card companies have individually specific requirements that the Council must address in reporting suspected or confirmed breaches of cardholder data. It will be the responsibility of the Town Clerk / Deputy Town Clerk to ensure these are addressed.

Policy Review
The Town Clerk is accountable for monitoring and reviewing this policy. This Policy was last reviewed in September 2023.

APPENDIX A

WOODLEY TOWN COUNCIL’S IT INFRASTRUCTURE

The information in this appendix should be considered in conjunction with the Council’s Disaster Recovery Plan.

The Council has two office/administration networks – one in the Council Offices at the Oakwood Centre and one at Woodford Park Leisure Centre. The networks are not linked with the exception of a data link for mutual back up of data between sites.

The Council Offices network is an Apple/Mac based network. A File Server and Mail server are located in the Archive Room with a PC server located in the main office.

The PC server houses the data from the Rialtus (RBS) software packages – Omega, Bookings and Allotments. This data is stored in this way as the RBS packages are not Mac compatible. The backed-up data on this server is however backed up to the Mail Server and Cloud storage.

Mac machines requiring the RBS software packages are equipped with ‘Parallels’ software, which creates a ‘virtual’ Windows PC within the Mac environment. This enables the RBS packages to be operated on these machines.

A maintenance contract is in place with Dejac Associates for the Mac network, machines, servers, wi-fi and email accounts. A separate smaller contract is in place with ASAP computers for maintenance of the PC machines at Woodford Park Leisure Centre and the PC server at the Oakwood Centre.

Procurement

New and replacement IT equipment is purchased as required and added to the maintenance contract schedule. IT purchases are made by the Town Clerk or Deputy Town Clerk and equipment must be appropriate and compatible with the other equipment and software used in the Council.

Disposal

Arrangements for the disposal of IT equipment are made by the Deputy Town Clerk via a specialist waste contractor (R3 Environmental Solutions). This requires the certified destruction of hard drives and data storage.

GDPR

All contractors with access to Council held data sign a data processor agreement and have appropriate safeguards in place to securely store data as required under the GDPR.

Security

Individual machines are password protected; there is no public access to office networks at ether site. Public wi-fi networks are separate from the office wi-fi networks, which are also password protected.

Firewall

The firewall is a ZyXEL USG 60W enterprise grade next generation firewall. The Firewall is managed by Dejac Associates along with the IT network, hardware and software.

The firewall provides the following protection:

- Anti-malware protection
- Antivirus

- Anti-spam
- Content Filtering
- Intrusion Detection & Prevention
- Application Intelligence

All devices are protected from these threats while they are within the Council network.

Antivirus and IDP signatures are updated hourly from ZyXels subscription service.

Firmware for the ZyXEL USG 60W is updated manually when a new release is made available by ZyXel.

Equipment and Servicing – Council Offices

COUNCIL OFFICES / OAKWOOD CENTRE	
Equipment	
Machines	x9 Mac (running OS X El Capitan or later) x2 Laptops (running Windows 7/10)
Server	x1 mac server x1 mac mail server x1 PC office server (for RBS software)
Wi-Fi	Oakwood Centre public wi-fi (plusnet line) Woodley Town Council broadband (BT)
Service Contract / Maintenance	
Dejac Associates Limited [redacted]	Alternative contact in case of emergency: [redacted]
Rialtus Business Services – RBS [redacted]	Omega (Accounts) Bookings Allotments Planning
Cloud Backup	
Ceejay Software / Backup Intelligence [redacted]	

Equipment and Servicing – Woodford Park Leisure Centre

WOODFORD PARK LEISURE CENTRE	
Equipment	
Machines	x3 PC
Server	x1 PC server
Wi-fi	Public wi-fi (plusnet line) Office wi-fi (BT)
Other	x1 Mac-book (Maintenance Manager) x1 Mac-book (Leisure Services Manager)
Service Contract / Maintenance	
ASAP Computers [redacted]	PCs, server & network
Dejac Associates Limited [redacted]	Email accounts/issues Alternative contact in case of emergency: [redacted]
Rialtus Business Services – RBS [redacted]	Bookings software

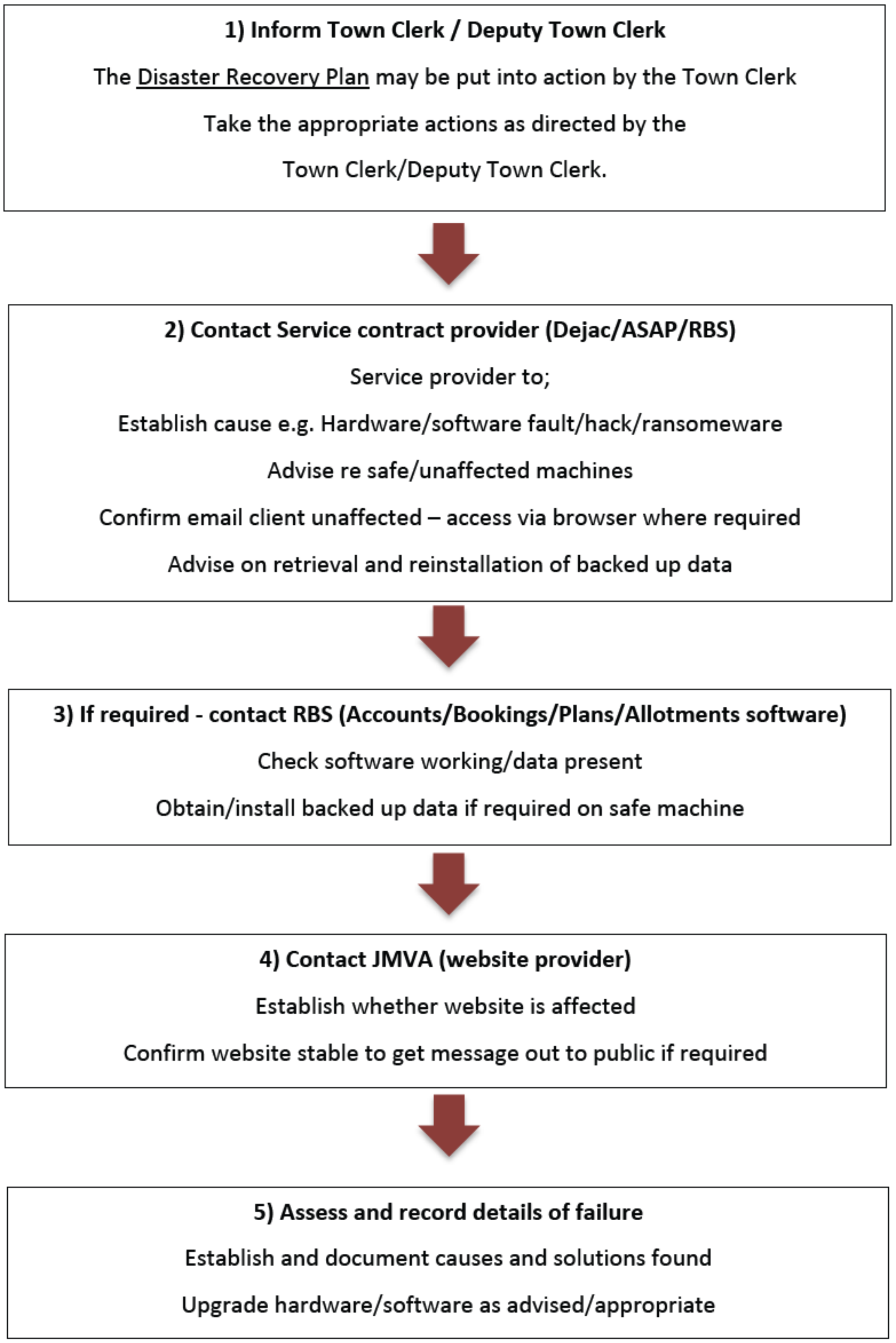
Data Backup

COUNCIL OFFICES / OAKWOOD CENTRE
• All Macs auto-backup daily to Mail Server (Mac Mini). Backup initiated when individual machines are turned on. • Mac File Server auto backed up daily to Mail Server. • Rialtus Suite (Bookings, Omega & Allotments Databases) backed up manually to PC Server weekly. • PC Server backed up daily to Mail Server. • All data backed up to Seagate drive on mail server – Daily. • All servers backed up to cloud – Daily.

WOODFORD PARK LEISURE CENTRE
• PCs auto-backup daily to PC server in back office • PC server auto-backup up daily to Oakwood Centre mail server • Mail server backed up to cloud daily

Network/system failure - actions

In event of a partial or complete IT network/system failure:



1) Inform Town Clerk / Deputy Town Clerk

The <u>Disaster Recovery Plan</u> may be put into action by the Town Clerk

Take the appropriate actions as directed by the
Town Clerk/Deputy Town Clerk.

2) Contact Service contract provider (Dejac/ASAP/RBS)

Service provider to;

Establish cause e.g. Hardware/software fault/hack/ransomeware

Advise re safe/unaffected machines

Confirm email client unaffected – access via browser where required

Advise on retrieval and reinstallation of backed up data

3) If required - contact RBS (Accounts/Bookings/Plans/Allotments software)

Check software working/data present

Obtain/install backed up data if required on safe machine

4) Contact JMVA (website provider)

Establish whether website is affected

Confirm website stable to get message out to public if required

5) Assess and record details of failure

Establish and document causes and solutions found

Upgrade hardware/software as advised/appropriate