WARSOP PARISH COUNCIL

RESERVES POLICY

Contents

Policy adopted: 14th September 2026

Minute Reference: FG-26-28a

Policy version reference: v1

Policy effective from: Immediately

Date for next review: September 2028

INTRODUCTION

Warsop Parish Council is required by statute to maintain financial reserves sufficient to meet the needs of the organisation. In addition, it has statutory limitations on how it spends certain receipts which it must ensure are accounted for separately to the council's general funds.

Whilst there is no statutory minimum (or maximum) level of reserves, the council should only hold general reserves for reasonable working capital needs or specific earmarked purposes. The Parish Council's Internal and External Auditors review the council's reserves and their justification annually. This policy sets out how the council will manage its General reserves (Contingency) and Earmarked Reserves (EMR).

POLICY AIMS

- Maintain an appropriate balance between holding excessive reserves and retaining a prudent level of funds
- Ensure reserves are held at an adequate and appropriate level for the Council's needs
- Rely on advice from the Responsible Finance Officer when determining the appropriate reserve levels, primarily during the budget setting process
- Avoid accumulating excessive reserves that could be seen as holding onto public monies unnecessarily
- Recognise the need to balance financial prudence with responsible financial management of precept funds
- Adopt a transparent and accountable approach to managing the Council's reserve levels as part of overall financial stewardship
- Maintain earmarked reserves (EMR) to save for and plan the maintenance and replacement of the Council's key assets, to ensure they are adequately funded and cared for over the long term.

DEFINITIONS

General Reserve

The General Reserve, also referred to as Contingency is not ringfenced (earmarked) for any specific expenditure, but is intended to cover the following working capital needs:

- To smooth the impact of uneven cashflow
- To cover unexpected/emergency expenditure
- To allow the Council to act in a flexible manner

The General Reserve will be replenished as part of the budget process in any year where it has been spent for unexpected/emergency expenditure.

Earmarked Reserves

The council may establish Earmarked (ringfenced) Reserves for any reason where it reasonably believes it may incur expenditure in the future. The council's current earmarked reserves include potential future election costs and maintenance. Any grant funding received for specific projects are 'ring-fenced' in certain reserves for specific expenditure not related to the general budget.

LEGISLATION AND GUIDANCE

The Local Government Act 1972, Section 111, supports the ability to adopt a Reserves Policy as part of responsible financial management. The Local Government Finance Act 1992, Section 32 requires local authorities to calculate their budget requirement, which includes the provisions for reserves. Section 43 requires precepting authorities (including Parish Councils) to determine the amount of their precept, which relies on understanding reserve levels.

Governance and Accountability for Smaller Authorities in England by the Joint Panel on Accountability and Governance (JPAG) or (SAPPP).

This guidance recommends adopting a Reserves Policy and provides advice on appropriate reserve levels. The most recent publication (2026) is cited in this policy.

The Good Councillor's Guide to Finance and Transparency by the National Association of Local Councils (NALC).

This guide for local councillors emphasises the importance of maintaining appropriate reserve levels and having a clear Reserves Policy. In the Annual Governance and Accountability Return – Annual Governance Statement, the Council asserts; "We have put in place arrangements for effective financial management during the year, and for the preparation of the accounting statements." To warrant a positive response, the Council needs to have regard to the need to put in place a Reserves Policy and have reviewed the level and purpose of all Earmarked Reserves.

RECOMMENDED LEVELS

It is essential that the Parish Council has sufficient reserves (general and earmarked) to finance both the day-to-day operations and future plans. The Parish Council has no specific right to accumulate funds via the precept. Therefore, all reserves should be reviewed and justified regularly (i.e. at least annually). It is good practice to transparently publish both the level and rationale of all reserves.

The Joint Panel on Accountability and Governance (JPAG) Practitioners' Guide or SAPPP sets out the 'proper practices' for how the council must maintain its accounts, recommends that the minimum level of general reserves (contingency) should be between three and twelve months of net revenue expenditure.

Net revenue expenditure is defined as precept, less amounts included in precept for loan repayment, capital projects and transfers to reserves. For an authority of Warsop Parish Council's size, an amount of 25-50% should be considered appropriate. The above recommended minimum level does not affect the level of earmarked reserves and/or capital receipts reserves that may or should be held by the Council. There is no upper limit to earmarked reserves, only that they must be held for genuine and identifiable purposes and projects, and their level should be subject to regular review and justification (at least annually and at budget setting) and should be separately identified and enumerated. Should a Council have significant levels of earmarked reserves, this would give rise to enquiries from internal and/or external auditors.

GENERAL RESERVES (CONTINGENCY)

General Reserves are often referred to as the "working balance", money which is not earmarked for specific purposes but rather sums of money held in anticipation of uneven cashflow or set aside to deal with unexpected events or emergencies. This is usually created through surpluses as a result of activities being postponed, cancelled or coming in under budget. Reserves of this nature can be spent or earmarked at the discretion of members, subject to approval by the Full Council. In assessing the level of the Warsop Parish Council's general reserves, account needs to be taken of the risks facing the Council in terms of any significant unforeseen expenditure requirements. This could include:

- Loss of staff, including long-term sick, and the potential requirement for interim staff
- Insurance claims not met
- Higher than expected election, and/or by-election costs
- Unanticipated legal costs
- Risks associated with inflation and cost of living crisis
- Funding the repair and replacement of assets
- Higher than expected debtors
- Natural disasters or extreme weather events causing damage to Council property and infrastructure
- Cyber-attacks or IT system failures disrupting Council operations
- Changes in legislation or regulations requiring unplanned expenditure
- Reductions in external funding sources.

Further major elements which could impact adversely on future precepts are:

- Capping of Warsop Parish Council's precept by Central Government
- Devolved services.

The optimum level for the General Reserve is determined by an assessment of the Council's potential exposure to financial risks. The level of contributions will be determined annually, taking account of the impact on council taxpayers, the availability of surpluses, and the level of earmarked reserves. The optimum level of General Reserves should be kept in the order of 25-50% of the Annual Precept minus capital expenditure and wholly discretionary expenditure.

The General Reserve shall not be allowed to decrease to a figure less than 30% of routine budget expenditure as this will expose the Council to the risk of not being able to meet unforeseen costs.

EARMARKED RESERVES

Earmarked Reserves will be established on a "needs" basis in line with anticipated requirements. Earmarked Reserves will increase through decisions of the Council and will decrease as they are spent on their specific intended purposes. The purpose of an Earmarked Reserve is to set aside amounts for projects that extend beyond one year or as a contingency against a specific situation occurring. Once an Earmarked Reserve has been established by the Town Council it is the responsibility of the Responsible Financial Officer to ensure funds are spent in line with their purpose. The purpose of each Earmarked Reserve should be reviewed annually to ensure that it is still relevant. If a specific reserve is no longer considered relevant or there is an overriding financial requirement to fund a priority elsewhere virement can be considered. Expenditure from Earmarked Reserves, or virement can only be authorised by the Full Council.

All Earmarked Reserves are recorded in the accounting software separately, updated by the Responsible Financial Officer. This lists the amounts, and the purpose they are held for, including any plan to increase reserves to meet future expected needs.

CONCLUSION

This Reserves Policy sets out the Parish Council's approach to maintaining an appropriate level of financial reserves to support our operations and fulfil our responsibilities to the local community. By adopting this policy, the Council commits to:

- Regularly reviewing the adequacy and purpose of both its general contingency reserves and earmarked reserves to ensure they continue to meet the identified needs
- Making transparent, evidence-based decisions when setting reserve levels as part of the annual budget process
- Utilising reserves judiciously and only for the intended purposes, with robust oversight and approval mechanisms
- Reporting on the state of the Council's reserves in its annual financial statements and other public communications, as required
- Aligning reserve management practices with relevant legislation, regulations, and sector guidance to demonstrate sound financial stewardship.

The Council recognises that maintaining appropriate reserve levels is crucial for its financial resilience and ability to deliver services effectively. This policy will be subject to regular review to confirm it remains fit-for-purpose and supports the Parish Council's strategic objectives.

Signature of the Chair: ____

Warsop Parish Council

INFORMATION TECHNOLOGY (IT) POLICY

Contents

Policy adopted: 14th September 2026 Minute Reference: FG-26-28b

Policy version reference: v2

Policy effective from: Immediately

Date for next review: September 2028

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Councils will also need to determine and clearly state whether limited personal use of IT equipment is permitted (for example, checking personal email or online shopping during lunch breaks).

Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Computer use

HARDWARE

1.1.1 Parish Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the Parish Council). Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

1.1.2 Locking computers when leaving desk, all councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

1.1.3 All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

1.1.4 Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

1.1.5 All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

1.1.6 Equipment should not be dismantled or reassembled without seeking advice.

1.1.7 Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software). Unless previously authorised.

1.1.8 Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Clerk

1.1.9 The council has a wireless network. Using a portable device to make personal Wi-Fi hot spots which bypass existing WiFi is not allowed.

1.1.10 Any faults or necessary repairs must be reported to the Clerk.

Equipment

PORTABLE EQUIPMENT

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.1.2 It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

2.1.3 All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.

2.1.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

2.1.5 Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods—for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

2.1.6 If an item of portable equipment is lost or damaged this should be reported to the Clerk. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet some of the costs for the loss/damage.

2.1.7 To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises, without the prior written permission of the Clerk. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

2.1.8 Under no circumstances should any non public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

2.1.9 In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the Clerk.

USE OF OWN DEVICES

2.2.1 The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's network or to store data on the council's server(s) or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

2.2.2 However, the same security precautions apply to personal devices as to the council's desktop equipment. For continuity purposes, calls made to external parties should (where possible) be made on council landlines or mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

2.2.3 Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice). For Workers or Contractors, we may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

2.2.4 In cases of legal proceedings against the council, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

2.2.5 Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.2.6 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a pin or finger print to protect their device(s) from being accessed.
- configure their device(s) to automatically prompt for a password after a period of inactivity
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email);
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from council data where possible;
- ensure secure WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.7 Personal data should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

2.2.8 Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

2.2.9 If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

2.2.10 Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use. Additional risks include data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

2.2.11 Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

2.2.12 Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to allow the Clerk access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.13 Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

Health and safety

3.1.1 Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.

3.1.2 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment.

3.1.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Clerk or the Chair of the HR Committee.

If any hazards are detected at a workstation, including ‘noises’ from the IT equipment, this should be reported immediately to the Clerk or the Chair of the HR Committee.

Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider.

- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

4.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chair in a sealed envelope, only to be accessed in an emergency.

4.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using a council-approved, encrypted password manager (e.g., LastPass, Bitwarden, or KeePass).

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorized passwords will be treated as a security incident.

4.1.6 Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.

The IT security provider is responsible for:

- Managing system/service credentials.
- Enforcing password policies. Auditing and monitoring password-related security practices.

Monitoring

5.1.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

5.1.5 The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

5.1.6 Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

5.1.7 The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

5.1.8 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

5.1.9 Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

5.1.10 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

5.1.11 The council has software and systems in place that can monitor and record all internet usage. A daily log is kept of all activity, which details the names of all websites accessed, along with the date and time of access, by individual councillors, staff, and other authorised users.

5.1.12 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

5.1.13 Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

5.1.14 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

Remote working

6.1.1 Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home, different premises or any other different venue), as follows:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the devise does not clearly support these actions (for example at an internet café), council services should not be accessed from that device;
- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc;
- any data printed should be collected and stored securely;
- all electronic files should be password protected and the data saved to the council's system/services when accessible;
- papers, files or computer equipment must not be left unattended at a non council premises unless arrangements have been made with a responsible person at the non-council premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time;
- any data should be kept safely and should only be disposed of securely;
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed;
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft;
- Councillors, staff, and other authorised users who work away from the office with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

6.1.2 Those issued with a 'dongle' to enable internet access from a laptop via 3G or 4G networks whilst away from their normal workplace should note that the cost of internet access can be very high. Dongles should therefore be used for essential council purposes only, especially if abroad.

6.1.3 Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

7.1.2 On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

7.1.3 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask the Clerk rather than assuming they know the right answer.

7.1.4 All councillors, staff, and other authorised users who need to use email as part of their role will normally be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

7.1.5 Email messages sent on the council's account are for council use only. Personal use is not permitted.

Use of the Internet

COPYRIGHT

8.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

8.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

8.1.3 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

8.1.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

8.1.5 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Clerk if unsure about anything.

TRADEMARKS, LINKS AND DATA PROTECTION

8.1.6 The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the Clerk.

8.1.7 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's Data Protection Policy.

ACCURACY OF INFORMATION

8.1.8 One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

Use of social media

9.1.1 Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

9.1.2 Personal use of social networking/media and chat sites should be restricted to breaks during working hours, or after hours with permission.

9.1.3 The council recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable.

However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors, staff, and other authorised users should be aware that parishioners or other local organisations may read councillors, staff, and other authorised users' personal weblogs, to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.

9.1.4 To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups,

suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of Warsop Parish Council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council.") Writers must not claim or give the impression that they are speaking on behalf of the council.

- The council expects councillors, staff, and other authorised users to be respectful about the council and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.
- Photos or videos that include employees or other workers wearing uniforms or clothing displaying the council's name or logo should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues, or the council. Additionally, photos, videos, or audio recordings must not be taken on council premises without explicit permission
- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations should not take place on any social networking sites, including forums.
- Any writing about or displaying photos or videos of internal activities that involves current councillors, staff, and other authorised persons, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff, and other authorised users anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.
- Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other councillors, staff, and other authorised users can raise grievances for alleged bullying and/or harassment.

- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the council, should be referred to the Clerk
- Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors, staff, and other authorised users who use X.com, LinkedIn, or other social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff, and other authorised users on LinkedIn, Facebook, X.com or any other social media/networking sites.
- During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor, member of staff, or other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

9.1.5 Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

9.1.6 It is important to note that personal contact details and information remain the property of the council. In addition, councillors, staff, and other authorised users leaving the council will be required to delete all council-related data including contact details from any personal device/equipment.

Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

End of Policy.

Signature of the Chair: ____________________________________

WARSOP PARISH COUNCIL

MANUAL HANDLING POLICY

AND

MANUAL HANDLING RISK ASSESSMENT

Policy adopted: 14TH SEPTEMBER 2026 Minute Reference FG-26-28

Policy version reference: v1

Policy effective from: Immediately

Date for next review: September 2028

Warsop Parish Council follows the Health and Safety Executive guidelines for lifting and no employee must lift over 25kg without assistance.

The Manual Handling Operations Regulations 1992 (MHOR) (as amended 2002) apply to any means of transporting or supporting a load, including the lifting, pushing, pulling, carrying or moving thereof, by and or by bodily force.

A load includes any person or animal.

The main requirements are:

• Avoiding the need to lift and carry wherever possible

Regulation 4 of MHOR requires the employer to avoid the need for hazardous manual handling activities *"as far as reasonably practicable"*

• Assessing those operations that are unavoidable to determine the level of risk

Assessment should consider the task, the load, the individual the environment and any other factor that may influence safe lifting and handling (e.g. Personal Protective equipment)

• Introduce suitable controls to reduce the risk of injury to the lowest extent practicable.

The ways of reducing risk could include:

➢ Improving the environment

➢ Using mechanical aids

MOHR and Section 2 of The Health and Safety at Work etc Act 1974 require the employer to:

➢ Provide suitable information, instruction or training on safe lifting and carrying techniques.

Warsop Parish Council will therefore ensure that:

• Manual handling assessments are carried out where relevant, monitored and reviewed and records of these kept,

• Suitable information, instruction or training is provide to persons undertaking manual handling activities,

• Employees who undertake manual handling activities are suitably screened in relation to health and safety prior to undertaking the work,

• Employees adhere to safe systems of work • Investigate any incidents in relation to manual handling and take suitable remedial action

Employees of Warsop Parish Council must ensure that:

• They report any personal health conditions that may adversely affect their ability to undertake manual handling activities

• They follow any instruction or training provided in safe manual handling activities

• Their own health and safety is not put at risk from the manual handling activities they are undertaking

• Use any equipment provided to aid with manual handling responsibly, when trained to do so and report any fault with the equipment to the Council promptly,

• Report any problems or incidents related to the manual handling activities to the Council promptly.

General Rules to Remember to reduce your risk of injury:

If there is a need to lift or move anything manually:

• Reduce the amount of twisting, stooping and reaching

• Avoid lifting from floor level or above shoulder height, especially heavy loads

• Adjust storage areas to minimize the need to carry out such movements

• Consider how you can minimise carrying distances

• Assess the weight to be carried and whether you can move the load safety or needs any help – maybe the load can be broken down to smaller, lighter components.

Signature of the Chair: ____

Risk assessment on the next page.

Manual Handling Risk Assessment

Name of Council: Warsop Parish Council
Date of Assessment/Review: 4th September 2026
Approval:

Area of risk	People at risk	Risk Level H/M/L	Management of Risk Current Controls	Action taken/completed Future Controls
General – consider unsatisfactory posture, movement, excessive weight, lowering or lifting, unpredictable movements, repetitive?	Employees / Volunteers Members of the public	Low	Manual handling tasks limited Specific high risk manual handling tasks undergo individual task manual handling assessment. For example – difficult to grasp, sharp, hot, using stairs, heavy etc. Employees / Volunteers are instructed to seek assistance where necessary. Pregnant people or those with health problems should not life heavy items Manual handling aids are provided where identified as necessary – trolley, gloves etc.	Consideration to online manual handling course Internal delivery of manual handling completed July 2026
Office Activities (Injuries/Strains)	Employees / Volunteers Members of the public	Low	Contractors are asked to deliver supplies directly to site or suitable alternative location Adequate storage facilities are provided. DSE Workstation checklist completed – posture, height	Lone working policy in place for office and working at home

			Consider temperature, humidity, lighting, noise etc	
Halls / Events / Meetings	Employees / Volunteers Members of the public	Low	Smaller, lightweight tables are used. Trolley used for moving & stacking chairs where possible Tables and chairs are stored in stacks of reasonable size Lift with partner, bend with knees Tables fold to facilitate transportation in some halls	Manual handling internal session completed July 2026
Outdoor / Events	Employees / Volunteers Members of the public	Low	Mechanical handling aids provided to Employees / Volunteers where identified as necessary (through individual task manual handling assessment) Gloves and protective footwear worn. Employees / Volunteers are instructed to seek assistance where necessary Suppliers to deliver heavy goods to site of work if possible Weather – consider there may be slippery surfaces in winter, ice / ungritted areas	