

ASH PARISH COUNCIL

Dear Councillors, you are summoned to the Ash Parish Council Meeting on Monday 02nd February 2026 at Ash Pavillion.

Clerk to the Council.



The Parish Council Meeting will be held on Monday 02nd February 2026 commencing at 7pm to discuss and take decisions on Parish business as outlined on the Agenda.

Public Forum: Members of the public and press are welcome to join the meeting and are able to speak on any matter for up to 10 minutes during the Public Forum which will take place at the start of the meeting. If the matter is likely to take longer than 10 minutes, notice should be provided to the Clerk by 12 noon on the Monday preceding the meeting.

1. **Public Forum**
2. **Somerset Council, Councillor's Report: February 2026**
3. **Apologies for absence**
4. **Declarations of Interest**
5. **To approve and sign Minutes of the Parish Council Meeting held on 12th January 2026**
6. **Matters arising (other than those on the agenda)**
 - a. Newly consecrated Cemetery – update re fees/rules/regulations.
 - b. SID – location identification/what three words
 - c. Dog control/Public Spaces Protection Order/dog fouling & dog control.
7. **Finance:**
 - a. **To approve and sign the Bank statements** – January 2026 to date
 - b. **To approve and minute payment requests.**
 - c. **To approve and sign bank reconciliations** January 2026 to date
8. **Planning: Notification only:**

Proposal: Application for a Lawful Development Certificate for the existing stand alone wooden garage/shed.
Location: 2 Back Street Ash Martock Somerset TA12 6NY
Applicant: COLIN SYNNOCK
Application Type : Certificate of Lawful Use or Development
Application Number: 25/02897/COL
9. **Council matters: IT Policy** – to consider and adopt IT Policy in accordance with Assertion 10 (AGAR)
10. **Council Matters** Procurement Policy & Purchase Order – to consider and adopt Procurement Policy &

Clerk to the Council: Zannette Bougourd. Tel: 01935571050
Email: clerk@ash-somerset-pc.gov.uk

ASH PARISH COUNCIL

purchase order in accordance with Procurement Act 2023 & Procurement Regulations 2024

Payments for Authorisation:

SLCC	Clerk Membership fee (1/3)	74.80
CiLCA January	CiLCA hours/pkg/mileage	212.10
HMRC	CiLCA January	53.02
Elancity	SIDs(including VAT £936)	5615.98

Signed:.....Date:

The Council is recommended to resolve that under section 1, paragraph 2 of The Public Bodies (admission to meetings) Act 1960, the press and public be excluded from the meeting for the following items of business because publicity would be prejudicial to the public interest by reason of the confidential nature of the business to be transacted.

Parish Matters - Grounds Maintenance / lengthsman contract – consider quotes.

Parish matters -Website content.

ASH PARISH COUNCIL

Minutes of the meeting held on 12th January 2026 (postponed from 05th January 2026) @ 7pm at Ash Pavillion, Ash Parish

Present: Cllr Steve Davey, Chairman, Caz Halfhide, Vice Chairman, Cllrs Tim Groves, Zac England, Antoinette Groves, Alan Britten & Marysia Trebley.

One member of the public was present for the first part of the meeting.

25/214 Public Forum. Noted that dog control in Millennium Wood has improved slightly since placing of sign advising dog control. Cllr A Groves noted that Somerset Council were continuing their consultation to update dog control legislation in public places. The wood manager is actively engaging with SC to represent Ash PC's areas of concern, including Millennium Wood, Recreation Ground, Churchyard and Cemetery. The next Somerset Council PSPO (Dog Control) meeting is on the 19th January 2026.

25/215 Somerset Council, Councillor's Report: January 2025. Report was received on 12th January, noted.

25/216 Apologies for absence. Cllrs J Bailey & E Pearlstone sent apologies.

25/217 Declarations of Interest. None declared.

25/218 To approve and sign Minutes of the Parish Council Meeting held on 03rd November 2025. Approved and Signed.

25/219 To approve and sign Minutes of the Parish Council Meeting held on 01st December 2025. Approved and signed.

25/220 Matters arising (other than those on the agenda)

- a. Role Allocation & Responsibilities. Cllr A Britten has agreed to take over the duties indicated from Cllr A Groves – Clerk will update list.
- b. Newly consecrated Cemetery –noted watering system may be malfunctioning, some hedging plants appear to have died – Cllr Davey will action.
- c. SID – locations. Cllrs England, Britten & Davey will meet on site to note proposed sites.

25/221 Finance:

- d. **To approve and sign the Bank statements** – December 2025 to date. Approved and signed.
- e. **To approve and minute payment requests.** Approved and signed
- f. **To approve and sign bank reconciliations** December 2025 to date. Approved and signed.
- g. **To approve payment requests.** – Approved and signed.

25/222 Budget: to approve the Budget for 2026/27 and authorise precept request. Note: Somerset Council have advised that payments for precepts over £10,000 will be made in April & September for the next financial year. Budget and precept request approved unanimously – Clerk to send precept request to SC.

Payments for Authorisation:

05/01/26	Lengthsman Nov 2025	£235.00
05/01/26	CiLCA – course textbook	£50.00
05/01/26	CiLCA Dec hrs/mileage/pkg	£212.10
05/01/26	HMRC - CiLCA	£53.02
05/01/26	Pavillion supplies	£27.74

Clerk to the Council: Zannette Bougourd. Tel: 01935571050
Email: clerk@ash-somerset-pc.gov.uk

ASH PARISH COUNCIL

Invoice received after publication of agenda:

Extra insurance premium re SIDs £34.09

The Council is recommended to resolve that under section 1, paragraph 2 of The Public Bodies (admission to meetings) Act 1960, the press and public be excluded from the meeting for the following items of business because publicity would be prejudicial to the public interest by reason of the confidential nature of the business to be transacted.

Parish Matters - Millennium Wood: Signage and usage review. See item 25/214

Historic incident noted, since that time the membership of the Parish Council has changed and now endeavour to be more proactive if and when incidents within the Parish occur. Noted that the PC have installed updated signage at the Millenium Wood and continue to engage with Somerset Council regarding the consultation to consolidate Public Space Protection Orders across Somerset. (Dog Fouling and Dogs on Leads). Suggested that a standing Agenda item is added: Parish Matters (incident reporting).

Parish Matters - Grounds Maintenance / lengthsman contract – review. Cllr A Groves noted that further quotes must be obtained before a decision was made. The PC has received one quote to date from the current contractor; Somerset Council declined to quote – they no longer provide grounds maintenance or lengthsman services. Clerk will endeavour to obtain further quotes.

Meeting closed @ 20.45hrs.

Next meeting 02nd February 2026

[illegible]

Parish/Town Council Notification

20 January 2026

Dear Sir/Madam

Proposal: Application for a Lawful Development Certificate for the existing stand alone wooden garage/shed.

Location: 2 Back Street Ash Martock Somerset TA12 6NY

Applicant: COLIN SYNNOCK

Application Type : Certificate of Lawful Use or Development

Application Number: 25/02897/COL

The Council has received the above application and the documents are available on the website : [Planning Search \(somerset.gov.uk\)](http://PlanningSearch(somerset.gov.uk))

This is a **notification only** and in line with the Council's Constitution and the adopted scheme of delegation and terms of reference, the decision for this application is delegated to officers. This notification is therefore being provided as a matter of courtesy for your information.

The application is being dealt with by Jacqui Churchill (Planning Officer) who can be contacted by email at jacqui.churchill@somerset.gov.uk or by telephone on Tel No: (01935) 462158

Please note that, for applications for Prior Approval/Notification and works to Trees in a Conservation Area, due to the tight timescale within which a decision needs to be made, and the deemed approval status of the application if the timescale is not met, a decision may need to be made very soon after you have received this notification.

This application is for a Certificate of Lawfulness and if you have evidence to contradict or otherwise make the applicant's version of events less than probable, then you can submit this information to the Council for consideration. Please be aware that this information will be shared with the applicant so that they can have an opportunity to comment on it and possibly produce counter-evidence.

Your response should be returned by email to (email address) . Please do not send direct to the Case Officer or include signatures or any other personal information that may need redacting.

Yours sincerely

Jacqui Churchill (Planning Officer)
Planning Team South
Somerset Council

ASH PARISH COUNCIL
IT POLICY
ADOPTED BY FULL COUNCIL FEBRUARY 2026
REVIEWED ANNUALLY.

Introduction

Each council will have its own IT setup and, as such, a single 'one-size-fits-all' IT policy is unlikely to be appropriate. Some smaller parish councils may operate with minimal equipment, while others may manage multiple devices connected to a central server. These guidelines are intended to help councils identify key considerations when developing or updating their own IT policy.

Councils that use external IT providers should ensure their policies accurately reflect current practices and contractual arrangements.

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 Ash Parish Council computer equipment is provided for council purposes; however reasonable personal use is permitted (reasonable interpreted as in the opinion of the clerk). 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 All councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to both council-owned and personal devices used for work. Failure to comply may result in 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, with precautions taken to prevent food or drink spills.
- 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 users are not to purchase any computer or mobile equipment (including software). Unless previously authorised.
- 1.1.8 Personal disks, USB sticks, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Clerk

1.1.9 All faults or necessary repairs must be reported to the Clerk

Equipment

2.1 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 disabled 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.

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.

2.2 Use of own devices

- 2.2.1 Personal laptops and other computers or other devices should not be brought into work and used to access council IT systems during working hours, unless this has been authorised by their line manager. This is to ensure that no viruses enter the system, to prevent time being wasted during working hours on personal use and to assist in maintaining security, confidentiality, and data protection.
- 2.2.2 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 website 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) 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.
- 2.2.3 However, the same security precautions apply to personal devices as to the council's desktop equipment. For continuity purposes, calls made to external parties must 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.

- 2.2.4 Councillors, staff, and other authorised users 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.
- 2.2.5 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.
- 2.2.6 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.
- 2.2.7 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:
- use a strong password or fingerprint to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after three failed login attempts.
 - configure their device(s) to automatically prompt for a password after a period of inactivity of more than 10 minutes
 - 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 and where possible ensure secure Wi-Fi 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.

2.2.8 Personal data relating to councillors, staff, and other authorised users, residents, and external stakeholders 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.

2.2.9 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. The following data must never be accessed or processed on a personal device :

- Personal contact details (names, addresses, telephone numbers, email addresses)
- Financial information (bank details, payment card information, payroll data)
- Health or medical records
- Sensitive personal data (relating to race, ethnicity, religion, sexual orientation)
- Criminal records or allegations
- Safeguarding information concerning children or vulnerable adults
- Commercially sensitive information (contracts, tenders, procurement details)
- Staff personnel files and disciplinary records
- Legal advice and correspondence
- Passwords, access credentials, or security information

Personal devices * include personal laptops, desktop computers, mobile phones, smartphones, tablets, iPads, USB drives, external hard drives, smartwatches, wearable devices, and home computers shared with family members.

- 2.2.10 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.
- 2.2.11 Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use. The Clerk will provide assistance or training in doing this if needed. 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.
- 2.2.12 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.
- 2.2.13 If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (<https://>). Unsecured wireless networks should not be used.
- 2.2.14 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 or IT services provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.
- 2.2.15 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. Further details are set out in the council's health and safety policy.

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

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Clerk.

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 of council], 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.

4.1.7 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 or user's email or 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.
- 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 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 device 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 “non council” premises unless arrangements have been made with a responsible person at a “noncouncil” 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.

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

8.1 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.

8.2 Trademarks, links and data protection

- 8.2.1 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.

- 8.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy.

8.3 Accuracy of information

- 8.3.1 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 are not permitted during working hours.
- 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 about the council 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:

9.1.5

- 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 the 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 with [residents and external stakeholders"] 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 staff, 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 or Communications Officer.
- 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

another authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

9.1.6 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.

9.1.7 It is important to note that resident and external stakeholder 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 resident and external stakeholders 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.

Guidance

Where there is text in [square brackets] this part may be updated or be deleted if not relevant. An alternative option may have been provided.

Important notice

This document was commissioned by the National Association of Local Councils (NALC) for the purpose of its member councils and county associations. Every effort has been made to ensure that the contents of this document are correct at time of publication. NALC cannot accept responsibility for errors, omissions and changes to information subsequent to publication.

Ash Parish Council

Procurement Policy

Introduction

The purpose of this policy is to provide guidance on the procedures which will be followed when purchasing goods and services. The policy aims to give effect to and comply with S135 of the Local Government Act 1972 and the Procurement Act 2023 & Procurement Regulations 2024.

Every contract shall comply with this Procurement Policy, the Council's adopted Standing Orders and Financial Regulations. These regulations cover, amongst other things: the number of quotations to be sought and the tendering procedure.

A contract is an agreement between the Council and an individual or organisation for the individual or organisation to provide works, goods or services (including the engagement of consultants) in exchange for payment by the Council. The following contracts are exempt from the requirements of these rules:

- contracts relating solely to disposal or acquisition of land
- employment contracts
- individual agency contracts for the provision of temporary staff
-

The Council strives to attain best value for the goods, materials and services that it purchases.

Best value is defined as a balance of price, quality of product and local supplier services. Before commencing a procurement, it is essential that the authorised person leading the procurement has identified the need and fully assessed the options for meeting those needs. The best use of purchasing power shall be sought by bulk purchases wherever possible.

Exceptions from any of the following provisions of these Contract Procurement Rules may be made under the direction of the Council, in consultation with the RFO, where they are satisfied that the exception is justified in special circumstances. Every exception and reason therefore shall be recorded by a resolution of Council.

The RFO and officers must be mindful of avoiding conflicts of interest when obtaining quotations and awarding tenders.

Quotations cannot be obtained by Members without prior approval of the RFO.

Purpose

Ash (Somerset) Parish Council's Procurement Policy has four main purposes:

1. To obtain best value in the way that the Council spends money, so that it may in turn offer better and more cost-effective services to the public.

2. To support the ability of the Council's officers to procure and manage goods, services and suppliers effectively, including informing all Council staff of the appropriate procedures and responsibilities.
3. To enable the Council to comply with legal obligations that govern the spending of public money.
4. To contribute to the Council's duty towards biodiversity and environmental aims.

Local contractors preferred

The Council recognises the benefits to the economy of using local businesses and will seek out local contractors and suppliers, wherever possible.

Competence of contractors and due diligence

The Council shall only enter into a contract with a supplier if it is satisfied as to the supplier's suitability, eligibility, financial standing and technical capacity to undertake the contract by carrying out appropriate due diligence.

All contractors and suppliers working on Council sites and/or projects will be required to comply with the Council's Health & Safety policy and any rules specific to the site of operation. Provision of suitable risk assessments and safe working method statements will be a condition of all such contracts. The Council requires all contractors working on Council sites and projects to maintain adequate insurance, including but not limited to Public Liability insurance for £10 million.

All procurement will be in accordance with the Council's Equality Diversity & Inclusion Policy and in line with legal obligations under the Equalities Act 2010 which makes it generally unlawful to discriminate on the grounds of colour, race, nationality, ethnic or national origins, sex or marital status, disability and on the grounds of age.

Equality and sustainability

The Council recognises the importance of sustainability and will take into account the environmental, social and economic impacts of its purchasing decisions.

The Council recognises its duty to protect biodiversity under Section 40 of the Natural Environment and Rural Communities (NERC) Act 2006. To meet this duty the Council will wherever possible purchase products that follow the Council's Biodiversity Policy.

The Council will encourage the purchase of locally sourced products and, where possible, ensure that products and materials originate from sustainable sources and accredited sustainable companies. In order to:

- minimise waste and maximise efficiency
- minimise travel
- minimise energy consumption
- promote greater use of new sustainable technologies
- keep material consumption to a minimum.

The Council will

- wherever possible, purchase goods that meet international Fairtrade standards (or similar).

- consider the whole life cost of products when selecting a supplier (Energy efficient products for example often have an increased capital cost that is more than offset over time by the reduced operational cost)
- never buy products that are harmful to the environment if a less damaging alternative is available (for example never use tropical hardwood that is not independently certified as being from a sustainable forest).
- always specify goods, products and materials that cause minimum damage to the environment including the impact of their manufacture, distribution, use & disposal.
- aim to promote sustainability within all its contract and tendering documentation and promote awareness amongst members and officers.
- continually review the purchasing of goods and services through contract specifications, with the intention of decreasing the Council's environmental impact and increasing its positive impacts on society, the local economy and producers.
- aim to draw the sustainable elements of its Procurement Policy to the attention of key suppliers and communicate it as widely as is practicable to the potential supply market.

Prompt payment of invoices

The Council understands the importance of paying suppliers promptly and will wherever possible settle accounts within a maximum of 30 days, or earlier, by agreement. In order to comply with current legislation all payments (apart from petty cash payments) are made by BACS transfer or Direct Debit.

Community engagement

Where relevant, the Council will consult with residents and service users to better understand what is needed, who will use it and what the essential requirements are for an item of capital expenditure.

Pre-approval of contractors

In respect of contracts that may be exempt from the Procurement Act 2023 the Council may require access to pre-approved contractors to supply routine services (or who can be called on to provide emergency services) including but not limited to:

- Electricians
- General builders
- Glaziers
- HR advice
- IT support
- Legal advice
- Locksmiths

- Plant hirers
- Play equipment repairers
- Plumbing and heating engineers
- Sextons
- Tree surgeons
- Vehicle and machinery service engineers

Best value

Normally the Council will accept the quotation, estimate or tender that provides best value for money. However, in accordance with Financial Regulations, the Council is not obliged to accept the lowest of any tender, quotation or estimate.

Purchases on account

The Council maintains monthly accounts with suppliers of regular purchases. All purchases on Council accounts may only be made by authorised Council officers who must be provided with a receipt. An official purchase order shall be issued for all work, goods and services above £500 excluding VAT unless a formal contract is to be prepared or an official order would be inappropriate. Limits will be set on each account on the maximum value of individual purchases and the overall balance on the account. Expenditure over these limits must be authorised in advance.

Specifications for tender process

Tendering processes ensure fair competition, achieve value for money and avoid anti-competitive behaviour. The tender process is detailed in Appendix 1 of the Council's adopted Financial Regulations.

Contracts

For contracts estimated to exceed £60,000 including VAT, the Clerk/RFO shall seek formal tenders from at least 3 suppliers agreed by Ash Parish Council.

For contracts estimated to be over £30,000 including VAT, the council must comply with any requirements of the Legislation regarding the publication of invitations and notices.

For contracts greater than £3,000 excluding VAT the Clerk/ RFO shall seek at least 2 fixed-price quotes;

where the value is between £500 and £3,000 excluding VAT, the Clerk/RFO shall try to obtain 2 estimates (which might include evidence of online prices, or recent prices from regular suppliers).

For smaller purchases, the clerk shall seek to achieve value for money.

Individual purchases within an agreed budget for that type of expenditure may be authorised by:

- the Clerk, under delegated authority, for any items below £500 excluding VAT.
 - the Clerk, in consultation with the Chair of the Council, for any items below £2,000 excluding VAT.
 - {in respect of grants, a duly authorised committee within any limits set by council and in accordance with any policy statement agreed by the council.}
 - the council for all items over £5,000;
- Such authorisation must be supported by a minute (in the case of council or committee decisions) or other auditable evidence trail.

(*The Regulations require councils to use the Contracts Finder website if they advertise contract opportunities and also to publicise the award of contracts over £30,000 including VAT, regardless of whether they were advertised.)

Contract variations

Any necessary instructions to vary a contract shall be made in writing by the RFO or persons responsible for supervising the contract. Where a variation occurs during the currency of the contract that is material and cannot be met from within the original contract sum an immediate report shall be made to the Council who shall decide what further action is necessary.

Termination of contracts

Council reserves the right to terminate any contract immediately where a supplier commits a material breach of the agreement to deliver services, or fails to deliver agreed services, in the agreed timeframe without a plan to address the failings.

Compliance with other relevant legislation

In cases where any law, statutory instrument of Government regulation is found to be at variance with any section of this policy, then that shall be applied, and this document shall be amended accordingly.

Appendix 1 - Tender process

- 1) Any invitation to tender shall state the general nature of the intended contract and the Clerk shall obtain the necessary technical assistance to prepare a specification in appropriate cases.
- 2) The invitation shall in addition state that tenders must be addressed to the Clerk in the ordinary course of post, unless an electronic tendering process has been agreed by the council.
- 3) Where a postal process is used, each tendering firm shall be supplied with a specifically marked envelope in which the tender is to be sealed and remain sealed until the prescribed date for opening tenders for that contract. All sealed tenders shall be opened at the same time on the prescribed date by the Clerk in the presence of at least one member of council.

- 4) Where an electronic tendering process is used, the council shall use a specific email address that will be monitored to ensure that nobody accesses any tender before the expiry of the deadline for submission.
- 5) Any invitation to tender issued under this regulation shall be subject to Standing Order [insert reference of the council's relevant standing order] and shall refer to the terms of the Bribery Act 2010.
- 6) Where the council, or duly delegated committee, does not accept any tender, quote or estimate, the work is not allocated and the council requires further pricing, no person shall be permitted to submit a later tender, estimate or quote who was present when the original decision-making process was being undertaken.

Adopted by Full Council at their meeting held on Monday 02nd February 2026

ASH (SOMERSET) PARISH COUNCIL

PURCHASE ORDER

Purchase Order Number:

Purchase Order Date:

Vendor's Name	Send To
	Zannette Bougourd, Clerk/RFO Ash (Somerset) Parish Council 9 Redgate Park Crewkerne TA197NL

Description of Items	Quantity	Unit Price	Total (£)
		Sub-total	
		VAT	
		Delivery	
		Other	
		Total (3)	

Comments or Special Instructions

If you have any questions about this Purchase Order, please contact Zannette Bougourd on 07471341433 /clerk@ash-somerset-pc.gpv.uk

Ash Parish Council

Procurement standard terms and conditions

STANDARD TERMS AND CONDITIONS FOR SUPPLY OF GOODS OR SERVICES TO ASH PARISH COUNCIL (SOMERSET)

1. BACKGROUND:

- 1.1 The Council wishes to be supplied with the Goods and/or Services.
- 1.2 The Council has selected you to supply the Goods and/or Services and you undertake to supply the same on the terms set out below.

2. DEFINITIONS:

- 2.1 "Applicable law" means applicable law of the United Kingdom (or a part of the United Kingdom);
- 2.2 "Commencement Date" means the date specified in the Purchase Order;
- 2.3 "Contract" means the Contract between the Council and You consisting of these terms and conditions and related Purchase Order but excluding Your terms and conditions of sale or supply;
- 2.4 "Contract price" means the price exclusive of any applicable Tax, payable to You by the Council as set out in the Purchase Order;
- 2.5 "Controller"; "Data Subject"; "International Organisation"; "Personal Data"; "Personal Data Breach"; "Processing"; and variations; "Processor" shall have the meanings given in applicable Data Protection Laws from time to time (and related expressions, including process, processed and processes shall be construed accordingly);
- 2.6 "Council" means Ash(Somerset) Parish Council;
- 2.7 "Data Protection Laws" means all applicable law relating to the Processing, privacy and/or use of Personal Data, as applicable to either party or the Services; including (a) the UK GDPR; (b) the Data Protection Act 2018; (c) the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426); and (d) any laws which implement or supplement any such laws;
- 2.8 "Data Protection Supervisory Authority" means any regulator, authority or body responsible for administering Data Protection Laws;
- 2.9 "Force Majeure Event" means any cause materially affecting the performance of the Services under the Contract arising from any act, events, omissions, happenings or non-happenings beyond the Parties reasonable control including, without limitation, acts of God, war, riot, fire, flood or any disaster affecting either of the Parties but will not mean any labour dispute between You and Your employees, agents or sub-contractors;
- 2.10 "Goods" means the goods to be supplied by You and specified in the Purchase Order;
- 2.11 "Prohibited Act" means:
 - (a) offering, giving or agreeing to give to any servant of the Council any gift or consideration of any kind as an inducement or reward:
 - (i) for doing or not doing (or for having done or not having done) any act in relation to the obtaining or performance of this Contract or any other contract with the Council; or

(ii) for showing favour or disfavour to any person in relation to this Contract or any other contract with the Council;

(b) committing any offence:

(i) under the Prevention of Corruption Acts 1889-1916;

(ii) under legislation creating offences in respect of fraudulent acts; or

(iii) at common law in respect of fraudulent acts in relation to this Contract or any other contract with the Council; or

(iv) defrauding or attempting to defraud or conspiring to defraud the Council;

2.12 "Processing End Date" means, in respect of any Protected Data, the earlier of (a) the end of the provision of the relevant Services related to the processing of such Protected Data; or (b) once processing by You of such Protected Data is no longer required for the purposes of Your performance or Your relevant obligations under this Contract;

2.13 "Protected Data" means Personal Data (as described in the Schedule) received from or on behalf of the Council, or otherwise obtained in connection with the performance of Your obligations under the Contract;

2.14 "Purchase Order" means the purchase order used by the Council to place an Order for supplies of Goods and/or Services;

2.15 "Services" means the services to be provided by You as identified in the Purchase Order;

2.16 "Staff" means all Your directors, officers, employees, agents, consultants and or those of any sub-contractor You engage in the performance of Your obligations under the Contract;

2.17 "Sub-Processor" means any Processor engaged by You (or by any other Sub-Processor) for carrying out any processing activities in respect of the Protected Data;

2.18 "UK GDPR" means the General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);

2.19 "Working Day" means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London;

2.20 "You" and variations including "Your" means the party supplying the Council with the Goods and/or Services.

3. DURATION

The Contract and the rights and obligations of the Parties shall take effect on the Contract commencement Date and shall continue until the expiry of the Contract Term or earlier termination of the Contract.

4. CONTRACT FOR GOODS

4.1 SPECIFICATION

(a) All goods shall be of the quality or kind mentioned in the Purchase Order but otherwise the goods shall be in accordance with any specification of the British Standards Institute, or EU equivalent, which relates to the goods and is current at the date of the quotation or tender. The goods shall comply with the requirements of any statute or subordinate legislation in force at the time of the delivery of the goods to the Council.

(b) You shall indemnify the Council against all loss, damage, costs and expenses for which

the Council is or becomes liable as a result of any infringement or alleged infringement by You of any third party's rights.

4.2 NOTICES

Any notice, request, demand, consent or approval given under or in connection with this Contract must be given in writing. Any such notice, request, demand, consent or approval shall be sent to the registered office or principal business address of either party and, if sent by post, shall be deemed to have been received on the second working day following the date of posting.

4.3 QUALITY ASSURANCE

(a) You shall give the Council access at all reasonable times to Your premises and allow them to inspect his quality systems and production methods and, if requested, to inspect, examine and test the Goods both during and after their manufacture and the materials being used in the manufacture.

(b) Any costs incurred by You in arranging compliance with the quality standards required by the Council shall be borne by You.

4.4 REJECTION AND REPLACEMENT

(a) Without prejudice to or limitation of its statutory rights the Council may within the Warranty Period, notwithstanding the use or continued use by the Council of the Goods after the right to reject them has arisen, reject by notice in writing (without liability to the Council) any Goods which, in the opinion of the Council are not of satisfactory quality and/or fit for purpose and/or not in accordance with the Purchase Order.

(b) Without prejudice to the Council's other rights and remedies, You shall in any event indemnify the Council against all costs and expenses incurred by the Council as a result of Your original supply of the rejected goods.

(c) You shall remove rejected Goods within 14 days of the date of the Council's notice of rejection, failing which the Council may (as it sole option) deliver them to You, in either case at Your cost and risk.

(d) Where such rejected Goods form part of a series of consignments, nothing in this Condition shall prevent the Council from accepting subsequent consignments if the Goods contained within such subsequent consignments are acceptable to the Council.

4.5 WARRANTY

Without prejudice to the Council's other rights and remedies, if during the Warranty Period, any defect occurs in any of the Goods due to the material, workmanship or design of the Goods not being in accordance with the Purchase Order or the Specification or any applicable statutory or regulatory standards, You shall as soon as practicable and in any event within a reasonable time as stipulated by the Council replace or repair such defective Goods at this own expense. Goods replaced or repaired under this Condition shall be subject to a fresh Warranty commencing on the actual date of delivery of the repaired or replaced Goods and continuing for the Warranty Period.

4.6 TITLE AND RISK

(a) Title in the Goods will pass to the Council upon payment to You, save where payment (either in whole or in part) is made for the Goods prior to their delivery to the Council, or where the Council has supplied materials to be incorporated in the Goods, in which cases Condition 4.7b) shall apply.

(b) Where under Condition 4.7a) this Condition 4.7b) (without prejudice to the Council's rights) title to the Goods shall vest in the Council from the commencement of their manufacture, and title to all materials and other items which You shall acquire or allocate for incorporation in any of the Goods shall vest in the Council from the time they are so acquired or allocated.

(c) The Goods shall be at Your risk until they are delivered to the Council notwithstanding that payment may have already been made and title passed to the Council, and You shall be responsible for any loss or damage and for arranging and paying for their storage, handling and insurance; the insurance shall be endorsed in the name of and protect the interests of the Council on an all risks basis and shall provide cover for loss or damage in transit.

5. CONTRACT FOR SERVICES

5.1 THE SERVICE STANDARD

You will at all times throughout the duration of this Contract:

(a) Provide the Services for the period specified in the Purchase Order in accordance with the Council's requirements as set out in the Purchase Order.

(b) Comply with the terms of this Contract.

(c) Exercise and continue to exercise the degree of skill, care and diligence reasonably to be expected of a skilled and competent provider of such services.

(d) Carry out all reasonable directions of the Council's representative.

(e) Use its reasonable endeavours to secure and achieve continuous improvement in the delivery of the Services during the Contract Term.

(f) Notify the Council in writing immediately on learning of any relationship or potential conflict of interest that might influence or be perceived to influence the provision of the Services.

6. PRICE AND PAYMENT

6.1 Ash (Somerset) Parish Council has committed to the UK Governments Transparency agenda (2010) by ensuring that ALL its expenditure over £500 along with a contract overview is made publicly available via the Council's website. Suppliers should be aware that the information published on a monthly/ quarterly basis includes the Suppliers Name, £ spend value, spend classification, contract start/ finish dates, total contract value. Commercially sensitive contract details/ price structures will not be published.

6.2 In consideration of the performance of Your obligation under the contract, the Council shall pay the price in accordance with the Contract.

6.3 The Council shall pay You the undisputed sums due in cleared funds within thirty (30) days of receipt and agreement of invoices, submitted monthly in arrears, for work completed to the reasonable satisfaction of the Council.

6.4 The Council may reduce payment in respect of any goods which You have either failed

to provide or have provided inadequate goods.

6.5 No increase in the Price may be made (whether on account of increased material, labour or transport costs, fluctuations in rates of exchange or otherwise) without the prior written consent of the Council.

6.6 Payment by the Council shall be without prejudice to any claims or rights which the Council may have against You and shall not constitute any admission by the Council as to Your performance of Your obligation hereunder.

7. INTELLECTUAL PROPERTY

7.1 Any specification supplied by the Council to You or specifically produced by You for the Council, in connection with the Contract, together with the copyright, design rights or any other intellectual property rights in the Purchase Order, shall be the exclusive property of the Council.

7.2 All designs, drawing, specifications and information supplied by Council in connection with the Contract are confidential, and their use must be strictly confined to Your own works for the purposes of the Contract. All such designs, drawings, specifications and information and all copies thereof must be returned to the Council on completion of the Contract.

7.3 You shall indemnify the Council against all actions, claims and demands, costs charges and expenses awarded against or incurred by the Council as a result of or in connection with any claim that the Goods or their use or resale infringes the patent, registered design, trademark, copyright or other intellectual property rights of any other person except to the extent that the claim arises from compliance with the Purchase Order.

8. STATUTORY RIGHTS

8.1 A party who is not a party to this Contract is not entitled to enforce any of its terms under the Contracts (Rights of Third Parties) Act 1999 except where this Contract expressly provides otherwise.

8.2 Without prejudice to or limitation of the Council's other rights, if You do not fulfil Your responsibilities and obligations under the Purchase Order You shall indemnify the Council against all costs for which the Council becomes liable and for which it would not otherwise be liable.

9. DATA PROTECTION

9.1 APPLICATION

- (a) This clause 9 applies if You are processing Personal Data on behalf of the Council.
- (b) You shall, comply with any notification requirements under the Data Protection Laws and both Parties shall duly observe all their obligations under the Data Protection Laws which arise in connection with the Contract.

9.2 CONFLICT

- (a) Unless otherwise expressly stated in this Contract:
 - (i) Your obligations and the Council's rights and remedies under this clause 9 are

cumulative with, and additional to, one another and those under any other provisions of this Contract; and

(ii) this clause 9 shall prevail over any other provision of this Contract in the event of any conflict.

9.3 COMPLIANCE WITH DATA PROTECTION LAWS

(a) The Parties agree that the Council is a Controller and that You are a Processor for the purposes of processing Protected Data pursuant to this Contract. You shall, and shall ensure the Sub-Processors and each of Your Staff shall, at all times comply with all Data Protection Laws in connection with the processing of Protected Data and the provision of the Services. Nothing in this Contract relieves You of any responsibilities or liabilities under Data Protection Laws.

(b) You shall indemnify and keep indemnified the Council against:

(i) all losses, claims, damages, liabilities, fines, interest, penalties, costs, charges, sanctions, expenses, compensation paid to Data Subjects (including compensation to protect goodwill and ex gratia payments), demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a Data Protection Supervisory Authority) arising out of or in connection with any breach by You of Your obligations under this clause 9; and

(ii) all amounts paid or payable by the Council to a third party which would not have been paid or payable if Your breach of this clause 9 had not occurred.

9.4 INSTRUCTIONS

You shall only process (and shall ensure the Staff only process) the Protected Data in accordance with the Schedule, this Contract and the Council's written instructions from time to time (including with regard to any transfer to which clause 9.8 relates) except where otherwise required by applicable law (and in such a case shall inform the Council of that legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest). You shall immediately inform the Council if any instruction relating to the Protected Data infringes or may infringe any Data Protection Law. You shall retain records of all instructions relating to the Protected Data received from the Council.

9.5 SECURITY

(a) You shall at all times implement and maintain appropriate technical and organisational measures to protect Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access. Such technical and organisational measures shall be at least equivalent to the technical and organisational measures set out in Part B of the Schedule and shall reflect the nature of the Protected Data.

(b) You may not make any change to the security measures You apply to the Protected Data to the extent any such change would conflict with the provisions of this Contract.

9.6 SUB-PROCESSING AND STAFF

You shall:

- (a) not permit any processing of Protected Data by any agent, sub-contractor, Sub-Processor or other third party (except Your own employees that are subject to an enforceable obligation of confidence with regards to the Protected Data) without the prior specific written authorisation of that third party by the Council that takes effect by way of a binding variation to this Contract and only then subject to such conditions as the Council may require;
- (b) ensure that access to Protected Data is limited to the authorised persons who need access to it to supply the Services;
- (c) prior to the relevant Sub-Processor carrying out any Processing activities in respect of the Protected Data, appoint the relevant Sub-Processor under a binding written contract containing the same obligations as under this clause 9 in respect of Protected Data and that (without prejudice to, or limitation of, the foregoing):
 - (i) includes providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing of the Protected Data will meet the requirements of all Data Protection Laws; and
 - (ii) is enforceable by You,and ensure each such Sub-Processor is at all times subject to a binding written contract which complies with such terms and that each Sub-Processor complies with all such obligations;
- (d) remain fully liable to the Council under this Contract for all the acts and omissions of each Sub-Processor and each of Your Staff as if they were its own; and
- (e) ensure that all persons authorised by You or any Sub-Processor to process Protected Data are reliable and:
 - (i) adequately trained on compliance with this clause 9 as applicable to the processing;
 - (ii) informed of the confidential nature of the Protected Data and that they must not disclose Protected Data;
 - (iii) subject to a binding and enforceable written contractual obligation to keep the Protected Data confidential; and
- (f) promptly provide all relevant details concerning, and a copy of, each Contract with a Sub-Processor to the Council on request.

9.7 ASSISTANCE

You shall (at Your own cost and expense) promptly:

- (a) provide such information and assistance (including by taking all appropriate technical and organisational measures) as the Council may require in relation to the fulfilment of the Council's obligations to respond to requests for exercising the Data Subjects' rights under Chapter III of the UK GDPR (and any similar obligations under applicable Data Protection Laws); and
- (b) provide such information, co-operation and other assistance to the Council as the Council reasonably requires (taking into account the nature of processing and the information available to You) to ensure compliance with the Council's obligations under Data Protection Laws, including with respect to:
 - (i) security of processing (including with any review of security measures);
 - (ii) data protection impact assessments (as such term is defined in Data Protection Laws);
 - (iii) prior consultation with a Data Protection Supervisory Authority regarding high risk

processing; and

(iv) any remedial action and/or notifications in response to any Personal Data Breach and/or any complaint or request relating to either party's obligations under Data Protection Laws relevant to this Contract, including (subject in each case to the Council's prior written authorisation) regarding any notification of the Personal Data Breach to Supervisory Authorities and/or communication to any affected Data Subjects;

(c) You shall (at no cost or expense to the Council) record and refer all requests and communications received from Data Subjects or any Data Protection Supervisory Authority to the Council which relate (or which may relate) to any Protected Data promptly (and in any event within 3 days of receipt) and shall not respond to any without the Council's express written approval and strictly in accordance with the Council's instructions unless and to the extent required by applicable law.

9.8 INTERNATIONAL TRANSFERS

You shall not process and/or transfer, or otherwise directly or indirectly disclose, any Protected Data in or to any country or territory outside the United Kingdom or to any International Organisation without the prior written authorisation of the Council (which may be refused or granted subject to such conditions as the Council deems necessary).

9.9 RECORDS AND AUDIT

You shall (and shall ensure all Sub-Processors shall) promptly make available to the Council (at Your cost and expense) such information as is reasonably required to demonstrate Your and the Council's compliance with their respective obligations under this clause 9 and the Data Protection Laws, and allow for, permit and contribute to audits, including inspections, by the Council (or another auditor mandated by the Council) for this purpose at the Council's request from time to time. You shall provide (or procure) access to all relevant premises, systems, Staff and records during normal business hours for the purposes of each such audit or inspection upon reasonable prior notice (not being more than 2 Working Days) and provide and procure all further reasonable co-operation, access and assistance in relation to any such audit or inspection.

9.10 BREACH

You shall promptly (and in any event within 24 hours):

(a) notify the Council if You (or any of the Sub-Processors or Your Staff) suspects or becomes aware of any suspected, actual or threatened occurrence of any Personal Data Breach in respect of any Protected Data; and

(b) provide all information as the Council requires to report the circumstances referred to in clause 9.10 to a Data Protection Supervisory Authority and to notify affected Data Subjects under the Data Protection Laws.

9.11 DELETION/ RETURN

(a) Subject to clause 9.11 (b) You shall (and shall ensure that each of the Sub-Processors and the Staff shall) within not less than 2 Working Days and not more than 4 Working Days of the relevant Processing End Date securely delete the Protected Data (and all copies)

except to the extent that storage of any such data is required by applicable law (and, if so, You shall inform the Council of any such requirement and shall securely delete such data as soon as it is permitted to do so under applicable law).

(b) You shall (and shall ensure that each of the Sub-Processors and Staff shall) promptly comply (in a secure manner) with any requests from time to time from the Council for the return or disclosure to the Council of any Protected Data in such form and by such manner as the Council reasonably requests, provided such request is received within 2 Working Days of the relevant Processing End Date.

9.12 SURVIVAL

This clause 9 shall survive termination or expiry of this Contract for any reason.

9.13 COST

You shall perform all Your obligations under this clause 9 at no cost or expense to the Council.

9.14 RIGHTS OF DATA SUBJECTS

Nothing in this Contract affects the rights of Data Subjects under the Data Protection Laws (including those in Articles 79 and 82 of the UK GDPR or in any similar Data Protection Laws) against the Council, You or any Sub-Processor.

10. FREEDOM OF INFORMATION

10.1 You recognise the Council's current and future obligations under the Freedom of Information Act 2000 and any codes of practice issued by the Government and the appropriate enforcement Agencies. You will comply with this legislation in so far as it places obligations upon the Council in the performance of its obligations under any contractual arrangement entered into. You will provide such assistance and support which may be requested from time to time by the Council for the purposes of enabling or assisting the Council to comply with the legislation.

10.2 In the event of a request made on the Council for access to information under the FOIA or any notice, recommendation or complaint made to the Council in relation to the FOIA, You will provide to the Council in relation to an access request, any details in respect of the information as the Council may request and a copy of the relevant information where the Council requests such copy; and in relation to any notice, recommendation or complaint, any background details, supporting documentation and copy information which the Council may request in order to deal with such notice, recommendation or complaint within 5 Working Days of the date of the request from the Council.

10.3 You acknowledge that the Council is obliged under the FOIA to disclose information, including information relating to its appointment under this Contract, to third Parties, subject to certain exemptions. You further accept and acknowledge that the decision to disclose information and the application of any such exemptions under the FOIA will be at the Council's sole discretion PROVIDED THAT the Council shall act reasonably and proportionately in exercising its obligations under the FOIA as to whether any exemptions

under section 43 of the FOIA may apply to protect Your legitimate commercial and trade secrets.

11. CONFIDENTIALITY

11.1 Subject to Clause 9 (Data Protection) and Clause 10 (Freedom of Information) You shall not, without the prior written consent of the Council, during or after the termination or expiry of this Contract disclose, directly or indirectly, to any person any information relating to the contract or the Council any information of whatever nature which is not in the public domain. Your obligations under this Condition shall survive the expiry or termination of the Contract for whatever reason.

12. DEFAULT

12.1 The goods may be rejected by the Council if they are not supplied and delivered by You when and as ordered by the Council, or, if the goods are not of the sort or quality contracted for, or if the goods are deficient in the quality or number charged for or stated in the delivery or advice note accompanying or preceding the goods. In such matter the decision of the Council shall be conclusive as against You. In every such case the Council may, without prejudice to any other remedy for breach of contract, employ any other person to supply the Council with the goods on such terms and conditions as the Council thinks fit for the remainder of the term of the Contract or any part thereof. In such cases it is hereby agreed that You shall pay the Council or the Council may deduct from any sum due or that may become due to You under the Contract or otherwise, all additional costs, charges or expenses incurred by the Council arising from Your default.

13. TERMINATION OF CONTRACT

13.1 The Council may terminate the Contract with immediate effect by notice in writing to You on or at any time after the occurrence of any of the following events:

- (a) the passing of a resolution for Your winding up or the making by a court of competent jurisdiction of an order for the winding up of You or Your dissolution;
- (b) the making of an administration order in relation to You or the appointment of a receiver or administrative receiver over, or the taking of possession or sale by an encumbrancer of a material part of Your assets;
- (c) the making of an arrangement or composition with Your creditors generally or making an application to a court of competent jurisdiction for protection from Your creditors generally;
- (d) You commit any Prohibited Act;
- (e) a breach of Your obligations to take out and maintain required insurances;
- (f) a material and substantial breach of any of Your obligations under this Contract.

13.2 In the event of the Council having the right to terminate under clauses 13.1 a), b) or c), the Council may, at its sole discretion, give the receiver, liquidator or other person (as appropriate) the option of carrying out the Contract subject to a guarantee acceptable to the Council being provided for the due and faithful performance of the Contract.

14. ASSIGNMENT AND SUB-CONTRACTING

14.1 You shall not assign, transfer sublet or sub contract the whole or any part of this contract without the prior written consent of the Council.

15. INDEMNITY AND INSURANCE

15.1 You shall indemnify and keep indemnified the Council against injury (including death) to any persons or loss of or damage to any property which may arise out of the act default or Your negligence, any sub-contractor or their respective employees or agents, and against all claims demands proceedings damages costs charges and expenses whatsoever in respect thereof or in relation thereto arising from the provision of the goods and/or Services.

15.2 You shall effect, with a reputable company, public and employer's liability and other insurances necessary to cover the risks contemplated by the Contract and shall at the request of the Council produce the relevant policy or policies together with receipts or other evidence of payment of the latest premium due thereunder. Public liability and Employers liability cover of at least £10 million shall be obtained, unless agreed otherwise with the Council. Where the Supply is a supply of consultancy services You shall maintain professional indemnity insurance during the Contract period and for 6 years afterwards to cover its liability to the Council under the Contract.

16. FORCE MAJEURE

16.1 Notwithstanding anything contained in these terms and conditions neither the Council nor You shall be liable for any loss damage or expense suffered or incurred by one party if by reason of a Force Majeure event or any restriction or prohibition imposed by the Government or any duly authorised authority which could not reasonably have been prevented or avoided by the Council or You as the case may be, either:

- (a) The Council is prevented from or delayed in accepting delivery of any goods or any part of a delivery or in paying for the same or any part of a delivery at the due time; or
- (b) You are prevented from or delayed in the supply of any goods ordered by the Council.

17. NO WAIVER

17.1 No delay, neglect or forbearance on the part of either party in enforcing against the other party any term or condition of the contract shall either be or be deemed to be a waiver or in any way prejudice any right of that party under this contract.

18. CORRUPT GIFTS AND FRAUD

18.1 As soon as either party becomes aware of or suspects the commission of any Prohibited Act in respect of the provision of the Services it will notify the other party.

18.2 In circumstances where a person employed by You is reasonably suspected of having committed a Prohibited Act You will provide to the Council such information as is reasonable to satisfy the Council that appropriate action has been taken to safeguard the Service Users or the Council.

19. ACCRUED RIGHTS AND REMEDIES

19.1 The termination of the Contract will not prejudice or affect any claim, right, action or remedy that will have accrued or will thereafter accrue to either party.

20. RIGHTS AND DUTIES RESERVED

20.1 All rights, duties and powers which the Council has as a local Council or which the Council's officers have as local Council officers are expressly reserved.

21. SURVIVAL OF TERMS

21.1 The terms of the Contract will (except in respect of any obligations fully performed prior to or at the completion of the Services) continue in force and effect after the completion of the Services by You.

22. ANTI-SLAVERY

22.1 In performing Your obligations under the Contract You shall:

- (a) comply with all applicable anti-slavery and human trafficking laws, statutes, regulations and codes from time to time in force including but not limited to the Modern Slavery Act 2015; and
- (b) not engage in any activity, practice or conduct that would constitute an offence under sections 1, 2 or 4, of the Modern Slavery Act 2015 if such activity, practice or conduct were carried out in the UK; and
- (c) ensure that each of Your sub-contractors and suppliers shall comply with all applicable anti-slavery and human trafficking laws, statutes, regulations and codes from time to time in force including but not limited to the Modern Slavery Act 2015.

22.2 You represent and warrant that neither You nor any of Your officers, employees or other persons associated with You:

- (a) have been convicted of any offence involving slavery and human trafficking; and
- (b) having made reasonable enquiries, so far as You are aware, have been or are the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence or alleged offence of or in connection with slavery and human trafficking.

22.3 You shall implement due diligence procedures for Your sub-contractors, and suppliers and other participants in Your supply chains, to ensure that there is no slavery or human trafficking in Your supply chains.

22.4 You shall notify the Council as soon as You become aware of:

- (a) any breach, or potential breach, of the applicable anti-slavery and human trafficking laws, statutes, regulations and codes from time to time in force; or
- (b) any actual or suspected slavery or human trafficking in a supply chain which has a connection with this Contract.

22.5 The Council may terminate the Contract with immediate effect by giving written notice to You if You or any of Your supply chain commits a breach of the applicable anti-slavery and human trafficking laws, statutes, regulations and codes from time to time in force.

23. LAW

23.1 This Contract shall be governed by and construed in accordance with English law and the Parties submit to the exclusive jurisdiction of the courts of England and Wales.

24. ENTIRE CONTRACT

24.1 This Contract is the entire Contract between the Parties and supersedes all representations, communications and prior Contracts between the Parties in that regard. Each party acknowledges that it has entered into this Contract in reliance only on the representations, warranties, promises and terms contained or expressly referred to in this Contract and, save as expressly set out in these terms and conditions, neither Party shall have any liability in respect of any other representation, warranty or promise unless it was made fraudulently.

SCHEDULE

PART A: DATA PROCESSING DETAILS

Processing of the Protected Data by You under this Contract shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Part A.

1. Subject-matter of processing: For the performance of the Services.
2. Duration of the processing: Processing shall take place until the Processing End Date.
3. Nature and purpose of the processing: All operations on the Protected Data as may be required for the performance of the Services only including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, erasure, destruction or other use.
4. Type of Personal Data: Name, address, date of birth, telephone number, email address or other Personal Data as may be processed in the performance of the Services.
5. Categories of Data Subjects: Council tenants, residents, members of the public, employees (including volunteers, agents, and temporary workers) or other categories of Data Subjects as may be required for the performance of the Services.

PART B: MINIMUM TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. Without prejudice to its other obligations, the You shall implement and maintain at least the following technical and organisational security measures to protect the Protected Data:
 - 1.1 In accordance with the Data Protection Laws, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Protected Data to be carried out under or in connection with this Agreement, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, You shall implement appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(1)(a) to 32(1)(d) (inclusive) of the GDPR.
 - 1.2 Without prejudice to Your other obligations, including as appropriate:
 - (a) encryption of data in transit by using suitable encryption solutions such as using https;

- (b) encryption of data at rest on all devices, including portable devices, using suitable encryption solutions;
- (c) only accessing data remotely using secure networks;
- (d) use of multi-factor authentication for internet facing systems;
- (e) timely decommissioning and secure wiping (that renders data unrecoverable) of old software and hardware;
- (f) secure disposal of hard copy documents;
- (g) completing regular software updates to all hardware and software;
- (h) real-time protection anti-virus and anti-malware software and web filtering on all systems;
- (i) firewalls and intrusion detection and prevention systems at the network edge;
- (j) the use of user access control management, including username and password restrictions, and audit logs;
- (k) enforcing unique passwords of sufficient complexity and regular expiry on all devices;
- (l) the use of data backup and disaster recovery measures and procedures;
- (m) procedures to ensure modifications to any systems, software or hardware are managed to ensure the ongoing confidentiality, integrity, availability of all data;
- (n) implementation of relevant policies covering Information Security, Data Protection, Bring Your Own Device, Acceptable Use and Clear Desk;
- (o) regular training of all Staff on confidentiality, data processing obligations, identification of Personal Data Breaches and risks;
- (p) suitable physical controls in place to protect data, networks and premises such as physical security on premises including reception or front desk, security passes, storage of documents in secure cabinets, secure disposal of materials, CCTV;
- (q) annual testing to assess and evaluate the effectiveness of the security measures set out in this paragraph 1.2 of this Part B.