To All Members of the Parish Council

You are hereby summoned to attend the Parish Council Meeting of Sacriston Parish Council at The Fulforth Centre on Wednesday, 4th March 2026, at 6.30 pm for the purpose of transacting the following business:

AGENDA

1. **Welcome and Apologies for Absence**
2. **Declarations of Interest -**To receive and record any Disclosable Pecuniary Interests in relation to items on the agenda.
3. **To consider the co-option of a Councillor to fill a casual vacancy** - To receive an application and, if appropriate, resolve to co-opt a Councillor to fill the current casual vacancy.
4. **Public Participation -** Questions and comments from members of the public (maximum 5 minutes per item/per individual).
5. **Approval of Minutes** - To approve the minutes of the meeting held on 4th February 2026 (attached)
6. **Police Matters**
7. **Planning Applications** - to receive and consider any response to applications received (attached).
8. **Growing Sacriston Together in Bloom**
9. **Parish Assets**
   a. Bus Shelters
   b. Village Clock
   c. Parish Building
   d. War Memorial
   e. Pit Wheel
10. **County Councillors' Reports** – to receive the information.
11. **Reports from Group Representatives**
    a. **Fulforth Centre** – To receive the verbal report provided.
    b. **HR and Finance Panel** - To receive the minutes from the meeting held on 5th January 2026.
    c. **Sacriston Allotment Association** – To receive the minutes from the meeting held on 5th January 2026.
12. **Finance Report**
    a. To review and approve payment of invoices received (attached).

13. **Parish Noticeboard** – To consider the report which was circulated at the meeting held on 4th February but deferred for further consideration (attached).

14. **Website Redevelopment and Email Management** – to consider the report (attached).

15. **Letter of Support – The Fulforth Centre** – to consider the request of providing a Letter of Support to The Fulforth Centre to apply for 106 funding for the replacement of a new roof.

16. **IT Policy** – to consider the policy (attached).

17. **Date and Time of Next Meeting** - Wednesday, 6th April 2026 at 6:30 PM

Signed: Mrs C Dixon (Clerk to the Council)

SACRISTON PARISH COUNCIL

Minutes of the meeting held on Wednesday, 4th February 2026 at 6.30 pm
In The Fulforth Centre

Present: Cllr H. Dixon (Chair), Cllr E Hopkins, Cllr A Page, Cllr K Wilson, Cllr E Waldock, Cllr R Sharp, Cllr G Ludlow, Cllr R Mickle, Cllr A Wray and Mrs C Dixon (Clerk)

Also, present was County Cllr T Robson

Apologies: Cllr D Cumiskey, Cllr M Morrell, Cllr G Ludlow, Cllr D Robson, and County Cllr J Pickard

The Parish Council wishes to record its sincere condolences to the family of Frank Morrell. Frank served as a Parish Councillor since 1979 and will be greatly missed.

Item No:

1. **Introductions and Apologies for Absence**
   The Chair opened the meeting at 6.30 pm and welcomed everyone.
   RESOLVED: To **NOTE** the apologies received.

2. **Declarations of Interest**
   RESOLVED: No declarations were received.

3. **To consider the co-option of a Councillor to fill a casual vacancy**
   Kim Welsh provided members with some background information about herself and why she would like to stand as a parish councillor.
   RESOLVED: To **APPROVE** the co-option of Kim Welsh as Parish Councillor. Kim then signed the Declaration of Acceptance of Office.

4. **Public Participation - (Questions & Comments from the public in attendance – max 5 mins per item/individual)**
   There was 2 members of the public in attendance.
   RESOLVED: There were no comments.

5. **Approval of Minutes**
   RESOLVED: The minutes from the Meeting held on 7th January 2026 were accepted and signed as a true record.

6. **Police Matters**
   RESOLVED: There were no comments.

Initials .....

7. **Planning Applications**
   DM/25/03524/FPA - Carina & Luis Nausner Carvalho
   23 Ashford Drive, Sacriston, Durham, DH7 6BB
   Removal of the existing porch and replace with a new porch with an enlarged entrance hall and W/C

   DM/25/02701/VOC - Langley Lodge Developments Limited
   St Peters Court, Sacriston, Durham, DH7 6FB HEADER
   Variation of Condition 2 (admissions policy) pursuant to planning permission

   RESOLVED: To **NOTE** no comments were received.

8. **Growing Sacriston Together in Bloom**
   Cllr Dixon provided an update about the flowers at the Crossroads.
   RESOLVED: To **NOTE** the update.

9. **Parish Assets**
   a. **Bus Shelters**
      RESOLVED: Nothing to report.
   b. **Village Clock** - The blue light at the top has stopped working.
      RESOLVED: To **APPROVE** the clerk to contact The Cumbria Clock Company to investigate the issue.
   c. **Parish Building**
      RESOLVED: Nothing to report.
   d. **War Memorial**
      RESOLVED: Nothing to report.
   e. **Pit Wheel**
      RESOLVED: Nothing to report.

10. **County Councillor Report**
    Cllr T Robson;
    - The roof at the WMC is in a state of disrepair. Funding will be required to replace the roof. Consideration has been given to moving into new premises.
    - The Fulforth Centre roof requires replacing, and 106 monies are to be applied for.
    - John Street carpark is a safety concern due to having no lighting. DCC will not put in any lighting as it is not adopted.
    - Update given on the final phase of Cross Lane development.
    - Working with Simon Hogg on matters and liaising directly with him.
    - Budget – happy to discuss if anyone has any questions.

    RESOLVED: To **NOTE** the verbal report.

11. **Reports from Group Representatives**
    a. **Fulforth Centre** – verbal report provided by Cllr Dixon.

Initials .....

RESOLVED: To **RECEIVE** the information.

b. **HR and Finance Panel**
RESOLVED: To **RECEIVE** the minutes of the meeting held on 1st December 2025.

c. **Sacriston Allotment Association**
RESOLVED: To **RECEIVE** the minutes from the Allotment Meeting held on 5th December 2025.

12. Finance Report

The Clerk updated members regarding the current bank account balance of £56,732.69.

a. To review and approve payment of invoices received.
RESOLVED: to **APPROVE** payment of the invoices.

13. Grant Application

Durham Hospitals Radio requested £500.
RESOLVED: To **APPROVE** the request of £500.

14. The Woodland Trust

RESOLVED: To **NOTE** the information.

15. Parish Noticeboard

RESOLVED: To **DEFER** until the next meeting, as members had not fully read the report provided.

16. Notice of Election

RESOLVED: To **NOTE** the information.

17. Festive Lights

Information provided regarding stress testing from DCC.
RESOLVED: To **NOTE** the information.

18. Date and Time of Next Meeting

The next meeting will be held on Wednesday, 4th March 2026, at 6.30 pm.

The meeting closed at 19.14pm.

Agreed and signed by Chair of Sacriston Parish Council .....

Date .....

Initials .....

Planning Applications

Week Ending 13th February 2026

DM/26/00247/FPA	Mr Behnam Azar	27 Uphill Drive Sacriston Durham DH7 6PP	Two storey side extension, application of render and window replacements

Agenda Item 11b

SACRISTON PARISH COUNCIL

HR and Finance Meeting

Minutes of the meeting held on 5th January 2026 at 6.30 pm
The Fulforth Centre

Present: Cllr H. Dixon (Chair), Cllr D Robson, Cllr E Waldock, Cllr A Page, and Mrs C. Dixon (Clerk)

Apologies: Cllr G Ludlow, Cllr R Sharp, and Cllr B Mickle

Item No:

1. **Welcome and Apologies for Absence -** The Chair opened the meeting at 7 pm and welcomed everyone.
   RESOLVED: To **RECEIVE** the apologies for absence.

2. **Declarations of Interest**
   RESOLVED: To **NOTE** there were no declarations of interest.

3. **Approval of Minutes**
   RESOLVED: To **APPROVE** the minutes of the meeting held on 1st December 2025 as a true and accurate record, and for the Chair to sign them accordingly.

4. **Finance Report**
   The clerk confirmed the current bank account balance as £61,757.00. The council had also received a VAT reclaim of £2,880.92.
   RESOLVED: To **NOTE** the finance report provided by the clerk.

5. **Precept**
   Members discussed the precept and budget for the 2026/2027 financial year. Several scenarios were reviewed in the report, including options to increase overall cash and raise Band D. After consideration, members agreed that a 12% increase in overall cash would be the preferred option. The Clerk advised that although this represented a 12% overall cash increase, the actual rise in Band D would equate to 15.57%. Members expressed concern that any higher increase would likely be unacceptable to residents. The Clerk further noted that, even with this proposed option, reserves could fall below the recommended level of between four and six months' expenditure. Members advised that this would be built up gradually over the coming years, should this be the case.
   RESOLVED: That it be recommended to Full Council that a precept of £73,530.42 be approved, equating to a Band D charge of £53.06.

6. **Invoices**
   RESOLVED: To **APPROVE** the invoices.

7. **HR**
   RESOLVED: To **NOTE** there was nothing to report.

8. **Date and Time of Next Meeting**
   RESOLVED: To **APPROVE** the meeting to be held on Monday, 2nd February 2026 at 6.30 pm

Meeting closed at 7.25pm.

Agreed and signed by Chair of HR and Finance .....

Date .....

SACRISTON PARISH ALLOTMENT ASSOCIATION

Minutes of the meeting held on 5th January 2026 at 6.30 pm
The Fulforth Centre

Present: Cllr H. Dixon (Chair), Cllr D Robson, Cllr E Waldock, Cllr A Page, and Mrs C. Dixon (Clerk)

Apologies: Cllr G Ludlow, Cllr R Sharp (Allotment Rep for Daisy Hill), and Cllr B Mickle (Allotment Rep for Cross Lane)

Item No:

1. **Welcome and Apologies for Absence -** The Chair opened the meeting at 6.30 pm and welcomed everyone.
   RESOLVED: To **RECEIVE** the apologies for absence.

2. **Declarations of Interest**
   RESOLVED: To **NOTE** there were no declarations of interest.

3. **Approval of Minutes**
   RESOLVED: To **APPROVE** the minutes of the meeting held on 1st December 2025 as a true and accurate record, and for the Chair to sign them accordingly.

4. **Gates/Boundary Fencing**
   Fencing at Cross Lane was discussed. The remaining wooden perimeter fencing is damaged and has come down; a section is missing next to P9 and the unused plot. It was queried if this section should have been replaced when the new metal fencing was erected, and if so, that the fencing company should be contacted. It was discussed whether the final wooden fence should be replaced with a metal fence, and then all fencing would be complete. The clerk did advise that there was a lot of money which had been spent on allotment fencing, and next year's budget allocation for fencing was £5,000.
   RESOLVED: To **APPROVE** contacting the Fencing Company for clarification on the missing section and to obtain a cost for renewing the remaining sections of the fence.

5. **Treasurer's Report**
   RESOLVED: Bank Account Balance: £2,272.77
   Cash in Hand: £60.00
   Gate Key Deposit Allocation: £620.00
   Total Available Funds: £1,712.77
   (Note: Gate Key Deposit is allocated and not available for general use)

6. **Water Rates**
   The Clerk advised that she had initially received correspondence stating that the monthly payments for Cross Lane would be nil due to a large credit balance on the

account. However, following the submission of a meter reading, the next bill showed the account to be in debit. The Clerk obtained a second meter reading to confirm the accuracy of the figures, which verified that the readings were correct. Members discussed the possibility of a leak, and it was agreed that Cllr Page would monitor the situation over the course of a week and provide the Clerk with the relevant information should a leak be suspected.
Daisy Hill Allotments: £115.53 (in debit)
Cross Lane Allotments: £414.08 (In debit)
RESOLVED: To **APPROVE** the clerk to contact the utility company if a leak is suspected.

7. **Matters Arising**
   RESOLVED: Nothing to report.

8. **Vacant Allotments**
   Vacant Plots Cross Lane: P19 and P20.
   Works Currently Underway On: Plots P14, P16, P17
   Daisy Hill: 0
   RESOLVED: To **NOTE** the vacant plots.

9. **Waiting Lists**
   Currently, there are 6 applicants on the waiting list for Cross Lane.
   There are 3 applicants on the list for Daisy Hill.
   RESOLVED: To **NOTE** the number of applicants on the waiting list and that the clerk was contacting people on the list and waiting for replies.

10. **Representative Reports**
    Cross Lane – Nothing to report.
    Daisy Hill – Nothing to report.
    RESOLVED: To **NOTE** there were no representative reports.

11. **Application for Buildings**
    RESOLVED: Nothing to report.

12. **AGM**
    The AGM and the AGM agenda were discussed.
    RESOLVED: To **APPROVE** a date for the AGM as Sunday 15th February 2026 at 3pm. To discuss items for the Agenda further at the next meeting and to bring the matter to Full Council for approval.

13. **Date and Time of Next Meeting**
    RESOLVED: To **APPROVE** the meeting to be held on Monday, 2nd February 2026 at 6.30 pm

Agreed and signed by Chair of Allotment Association.....

Date .....

Meeting Closed at 18.50pm

Report Email Management and Website

Purpose of the Report

The purpose of this report is to provide an update to the Council regarding:

- The use of personal email addresses by councillors for council business.
- An update on the council's website

Email Management

Currently, councillors do not have dedicated parish council email addresses and are using personal email accounts for council business. This practice is not recommended for several reasons.

Data Protection: Use of personal accounts increases the risk of breaching UK GDPR and the Data Protection Act 2018, particularly where sensitive or personal information is involved.

FOI and Subject Access Requests: Council correspondence held in personal accounts may be harder to identify and retrieve, creating risks in meeting statutory deadlines and demonstrating proper record management.

Record Keeping and Continuity: Personal email use can lead to inconsistent record retention and reduced transparency. Official accounts ensure communications are properly archived and remain accessible when councillors leave office.

Security and Oversight: Personal accounts are outside the Council's control and may lack appropriate security and administrative safeguards.

Professionalism and Public Confidence: Dedicated council email addresses promote transparency, accountability, and clear separation between council and private matters.

Website

The website is now significantly out of date in both design and functionality. There are concerns that it may not fully meet current accessibility requirements, including the Web Content Accessibility Guidelines (WCAG) 2.2 AA and the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018.

In its current format, the website is not as user-friendly as it should be. Navigation can be difficult, information is not always easy to locate, and the overall layout does not reflect modern website standards.

In addition, maintaining and updating the website is a time-consuming task. The Clerk requires additional support in managing the website, as this responsibility is difficult to accommodate alongside other statutory duties. There are also concerns that specialist knowledge is required to properly understand and implement current accessibility requirements, which the Clerk does not currently possess.

Recommendation

a) The Council approve the use of.gov.uk email addresses for all councillors.
b) The Council approve one of the quotes (Appendix A) to provide all.gov.uk email addresses.
c) The Council approve one of the quotes (Appendix A) for the redevelopment/renewal of the website.

Claire Dixon
Clerk to the Council

Quotes			
Name	**Information**	**Email Addresses only**	**Email and Website provider**
Parish Online	Current provider of clerks email address (clerk@sacristonparishcouncil.gov.uk) which is free.	Can provide up to 20 mailboxes with 5GB storage for councillors at a cost of **£260 ex VAT per annum.** This is with email provider Zoho.	Can provide a domain name for a website (gov.uk, up to 20 email addresses, website - which includes hosting, ongoing maintenance and upgrades, content migration, support, accessibility. **£490 ex VAT per annum** (websites can be ready in 4-6 weeks)
ALV IT Solutions	Current provider for hosting domain and website support	Microsoft Officer 365 Basic 50GB **£8 per user per month**	Website redevelopment **£400 one off** then would be the annual fees for domain hosting **£365 per annum**
CloudNext Sales		**£49.99 plus VAT** for 25 email addresses but are not able to have one account with someone else and then the rest with them so would need to move the clerks email address also.	Could not migrate the current Wix website and advised we would have to have a new one built first. Once built would charge **£49.99 plus VAT per annum** but this also includes email addressess. For the .gov.uk it would be **£50 plus VAT per annum.**
Eyelid Productions	Provider quote for a new website to be hosted by CloudNext Sales		To build a new website **-£949.99 inc VAT**

SACRISTON PARISH COUNCIL

INFORMATION TECHNOLOGY POLICY

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors and staff 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 and employees are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

Scope of this policy

This policy applies to all councillors and staff, 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

1.1 Hardware

1.1.1 Council computer equipment is provided for council purposes only.

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

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

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

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

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

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

1.1.8 Any faults or necessary repairs must be reported to the Council.

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 disenabled or removed.

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

2.1.6 If an item of portable equipment is lost or damaged, this should be reported to the Council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first £100 of the loss/damage.

2.1.7 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).

2.1.8 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 The Council recognises that some councillors and staff 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 computer or to store data on the council's server(s) or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

2.2.2 However, the same security precautions apply to personal devices as to the council's desktop equipment. For continuity purposes, calls made to external parties (such as external stakeholders) 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.

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

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

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

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

- use a 6-digit pin or fingerprint (preferably the latter) to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after 3 of failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 3 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 and staff are therefore advised to keep personal data separate from council data where possible;
- ensure secure WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the council or the clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.7 Personal 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 laptop, tablet, or mobile phone.

2.2.8 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.

2.2.9 Councillors and staff 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.

2.2.10 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.

2.2.11 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 and staff are required to allow the Chair to access the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.12 Councillors and staff 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 and staff 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 and staff 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 Council.

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

Password and Authentication Policy

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

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

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider.
- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

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

4.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.

- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel, with a copy provided to the Chair, in a sealed envelope, only to be accessed in an emergency.

4.1.3 Password Storage and Management

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

4.1.4 Password Change Requirements

- Immediately change the 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 unauthorised passwords will be treated as a security incident.

4.1.6 Responsibility

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

The IT security provider is responsible for:

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

Monitoring

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

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

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

5.1.7 The information obtained through monitoring may be shared internally, including with relevant councillors if access to the data is necessary for the 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 and staff 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 reserves the right to inspect all files stored on its computer systems in order to ensure 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.

5.1.12 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.

5.1.13 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, 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 any non council premises unless arrangements have been made with a responsible person at the 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 and staff 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 and staff 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 and staff 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 and staff as to what may and may not be done. If there is something which is not covered in the policy, councillors and staff should ask the Clerk, rather than assuming they know the right answer.

7.1.4 All councillors and staff 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 and staff 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 and staff 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, a copy of which is available from the Clerk.

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 The council recognises the importance of councillors and staff 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 external stakeholders or members of the public 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 and staff 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.

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

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of 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.
- Any employee who is developing a site or writing a blog that will mention the council, our current or potential plans, councillors, staff, and other authorised users, partners, must inform the clerk that they are writing this and gain agreement before going 'live'.
- The council expects councillors and staff to be respectful about the council and its current or potential councillors or clerk, 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 should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues, or the council.
- Comments posted by councillors and staff on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations with members of the public 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 and staff 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 and staff 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 and staff 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 its councillors/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.
- Councillors and staff 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 and staff 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 and staff who have left the council must not post any inappropriate comments about the council or its councillors and staff 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 or member of staff. All such contacts will be considered council property and may be subject to disclosure upon request.

9.1.4 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 and staff 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.

9.1.5 It is important to note that contact details and information remain the property of the council. In addition, councillors and staff leaving the council will be required to delete all council-related data, including all 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.