WESTON AND CREWE GREEN PARISH COUNCIL

Mark Robinson
Clerk to the Parish Council
Tel: 07835 556343
E-mail: clerk@westonandcrewegreen-pc.gov.uk

06 February 2026

NOTICE OF THE MEETING OF THE PARISH COUNCIL

Parish Councillors are summoned to a meeting to be held on:

Date: Thursday, 12 February 2026

Time: **7.00PM**

Venue: Weston Church Hall

Clerk to the Parish Council

Members of the Parish Council
John Densem (Chairman), Janet Chamberlain, John Chambers, John Cornell, Gillian Grocott, Alison Heler, Annelene Kiddie, Simon Lewis, and Chad Wilkinson.

Cheshire East Ward Councillors
Janet Clowes (Wybunbury), Steve Edgar (Haslington) and Alison Heler (Haslington)

MEMBERS OF THE PUBLIC ARE WELCOME TO ATTEND THIS MEETING.

A G E N D A

1. APOLOGIES FOR ABSENCE

2. DECLARATIONS OF INTEREST AND DISPENSATIONS
if a member is present at a meeting of the authority, and they have a disclosable interest in any matter to be considered or being considered at the meeting, they should disclose the interest to the meeting and follow the Council's code of conduct. Whilst the Clerk can offer guidance on the Code of Conduct, it remains the responsibility of the Member to decide whether they have an interest in a particular item. To consider any requests for dispensations

3. MINUTES OF THE PREVIOUS MEETING
To consider the minutes of the meeting held on 15 January 2026 (appended).

4. PLANNING MATTERS
The Chairman of the Planning Committee to update on
i) Neighbourhood Plan

ii) New National Planning Policy Framework – consultation (report to follow)
iii) Planning Update

1) Decisions by the Planning Committee

App No	Application	Decision
25/4770/HOUS	Installation of an Air Source Heat Pump at 8 Gorsty Hill Close, Balterley Heath, Crewe	No objection

2) Decisions by Cheshire East Council

App No	Application	Decision
25/2466/VOC	Variation of Condition 2 at Greenacre, 10a Cemetery Road, Weston	Approved
25/3788/HOUS	Two storey side extension and associated internal alterations at Stable House, Narrow Lane, Crewe	Approved
25/3999/FUL	Erection of building to provide for additional nursery floorspace, and all associated works at Crewe Nature Kindergarten, Weston	Approved

5. VILLAGE HALL COMMITTEE
To receive an update.

6. POLICE MATTERS
To note the Beat report (appended)

7. GOVERNANCE
- Assertion 10 (appended)
- Information Management and Technology Policy (appended)

8. CHESHIRE EAST COUNCILLORS' REPORTS
To receive reports from Cheshire East Ward Councillors

9. PARISH COUNCILLORS' REPORTS
Members are invited to report on any matters of interest to the Parish Council and to request items for inclusion on the next agenda.

10. OPEN FORUM – QUESTIONS FROM MEMBERS OF THE PUBLIC
In accordance with Standing Orders, members of the public are invited to ask questions or address the Parish Council.

11. FINANCE REPORT
To consider the:
- Payment and Income Schedule (to follow)

12. DATE OF NEXT MEETING
Thursday, 12 March 2026

WESTON AND CREWE GREEN PARISH COUNCIL
MINUTES OF THE MEETING HELD ON THURSDAY 15 JANUARY 2026

PRESENT:
Councillors: John Densem (Chairman), Janet Chamberlain, John Chambers, John Cornell, Gillian Grocott, Alison Heler, Annelene Kiddie, Simon Lewis and Chad Wilkinson.

IN ATTENDANCE:
Borough Cllr Janet Clowes.

25/088 APOLOGIES FOR ABSENCE
Cllr Broome.

25/089 DECLARATIONS OF INTEREST
None

25/090 MINUTES OF THE PREVIOUS MEETING
RESOLVED – that the minutes of the meeting held on 11 December 2025 be confirmed as a true and correct record.

25/091 PLANNING MATTERS
1) Neighbourhood Plan
Cllr Cornell advised that the Plan had been submitted to Cheshire East Council, which had commenced the Regulation 16 consultation that would end on 16 February 2026. The Plan would then be submitted to an Independent examiner and then go to referendum. It was expected that the process would be complete by "early spring".

2) National Planning Policy Framework (NPPF)
It was confirmed that the new NPPF had been released for consultation, with a deadline for comments of 10 March. It was suggested that a meeting be held with Cheshire East Council planning officers to discuss their views on the proposed changes.
RESOLVED – that the submission of the Parish Council's response to the consultation be delegated to the Clerk, in consultation with the Chairman and Vice-Chairman of the Planning Committee.

3) ONWARD/MUSE Liaison Meeting
Cllr Cornell provided feedback from the recent Liaison meeting, which related to this development off David Whitby Way. Concern was expressed at the submission of revised plans without Cheshire East Council undertaking further consultation.

There was clearly a need for a further meeting with planning officers, therefore, Borough Cllr Clowes would seek to arrange this. To support this, Cllr Cornell would provide a timeline of the developments on the site.

25/092 VILLAGE HALL COMMITTEE
The Chairman referred to a recent meeting with one of the remaining Committee members. There were a number of maintenance issues that would require resolution in the short term. There would also be an Open Committee meeting to encourage volunteers to join the Committee.

25/093 POLICE MATTERS
Councillors reviewed the Beat report for Wybunbury ward.

There had been discussion at the previous meeting regarding Cheshire Constabulary's proposal to reduce PCSOs across Cheshire from 87 to 27. Since the meeting, the Constabulary had confirmed that this would be proceeding, citing that

"reducing the number of PCSOs is essential to futureproofing the force, enabling us to balance our budget while maintaining our commitment to neighbourhood policing."

Borough Cllr Clowes provided a further update in that the Police and Crime Commissioner had agreed to fund 10 of the removed posts and would be seeking government approval to increase the precept by above the 5% limit to fund more. A consultation on this was currently open.

25/094 REPORTS OF CHESHIRE EAST COUNCILLORS

Borough Cllr Heler referred to forthcoming roadworks in the Parish Council area –

- Cemetery Road: 19, 20 and 26 to 30 January
- Englesea Brook Lane: 29 January
- Main Road: 21 January
- Poppy Close: 26-30 January
- East Avenue: 26-30 January

Borough Cllr Clowes referred to the diversion of one of the Public Rights of Way between Wychwood Village and Snape Lane. There was uncertainty as to who had undertaken the works and a response was awaited from Cheshire East Council.

25/095 PARISH COUNCILLORS' REPORTS

Councillors discussed the complaints regarding the road safety issues on Slaughter Hill, Crewe Green. It was noted that another 30-mph sign would be erected but the residents had requested any additional measures, which were being considered by the Borough Council.

It was noted that the Parish Council was responsible for the filling of grit bins across the Parish. It was suggested that additional grit bins be provided on East Avenue and Wychwood Village.

Concern was expressed regarding storage containers being placed on land adjacent to the Gorsty fishing lakes.

Cllr Wilkinson referred to the provision of real time information at bus stops, as discussed at the previous meeting. Cheshire East Council was currently out to tender for a borough-wide real-time information system, which would provide all of the functionality required to provide running information at any stop within the Borough. However, the funded provision of the display equipment would be limited to the hubs in the area. Outside of these areas, Parish Council would be invited to consider funding equipment in their areas, which would cost between £4,000 and £15,000 per installation.

25/096 OPEN FORUM – QUESTIONS FROM MEMBERS OF THE PUBLIC

No questions received.

25/097 FINANCE REPORT

1) Payments

RESOLVED – to note the payments approved in accordance with Financial Regulations and Payment Schedule

Payee	Reason	Gross £	VAT £	Net £
Unity Trust	Fees	6.00		6.00
Mark Robinson	Salary and Office Allowance (Nov)	1,319.40		1,319.40
HMRC	PAYE Q3	3,596.65		3,596.65
Scottish Power	Electricity	228.53	10.88	217.65

RESOLVED – to approve the following payment:

Payee	Reason	Gross £	VAT £	Net £
Kingfisher Direct	Rock salt	270.00	45.00	225.00
Border Tree Care	Felling of tree	180.00	30.00	150.00

2) Budget and Precept 2026/27

Councillors reviewed the recommendations from the meeting of the Finance Committee regarding the Budget and Precept 2026/27.

RESOLVED – that:-

i) The Council's budget be approved as recommended by the Committee in the sum of £82,953.40.

ii) The Council's precept be in the sum of £64,000 (an increase on 2.7%).

3) External Audit

The External Auditor has advised that "in our opinion the information in Sections 1 and 2 of the Annual Governance and Accountability Return is in accordance with Proper Practices and no other matters have come to our attention giving cause for concern that relevant legislation and regulatory requirements have not been met."

25/098 DATE OF NEXT MEETING

Thursday, 12 February 2026 commencing at **7.00pm**.

WESTON AND CREWE GREEN PARISH COUNCIL

MEETING: 12 FEBRUARY 2026

WYBUNBURY WARD CRIME DATA FOR JANUARY 2026
02/01/26. Property Found: Cobbs Lane Hough, replica firearm found at property, handed in to Crewe Police Station.
03/01/26. Harassment: Asphodel Road Shavington Park.
05/01/26. Theft: The Swan Wybunbury, theft of cooking oil.
07/01/26. Domestic Incident: Weston.
07/01/26. Violence/Harassment: Main Road Wybunbury, reports of an altercation outside a property.
08/01/26. Domestic Incident: Shavington park.
09/01/26. Fraud: Audlem Road Hatherton, reports of cloned number plates on a vehicle in Oxford.
11/01/26. ASB: Main Road Wybunbury, someone has loudly knocked on residents window.
13/01/26. Suspicious Activity: Wychwood Park, reports of a tent near the park possibly relating to recent burglaries, tent checked with no concerns.
14/01/26. RTC Damage Only: Checkley Lane Checkley.
14/01/26. Highway Disruption: London Road Doddington, an abandoned vehicle left in the road.
15/01/26. Highway Disruption: A529 Hatherton, temporary traffic lights not working.
15/01/26. Theft of Motor Vehicle: Weston, dispute over a borrowed vehicle that has not been returned.
16/01/26. Highway Disruption: London Road Bridgemere, vehicle has broken down in a dangerous position.
17/01/26. Suspicious Person: Ferndown Way Weston, males seen with torches in a field of Waybutt Lane. Officers attend , nobody found.
18/01/26. Suspicious Activity: Sundew Road, reports of the smell of cannabis from a property.
18/01/26. RTC: London Road Walgherton, low speed RTC but one driver had a medical episode and was taken to hospital.
19/01/26. Domestic Incident: Hough.
19/01/26. Violence/Harassment: Church Lane Hunsterson, caller walking in a field was approached by another male holding a screwdriver. Caller walked home with no other issues.
19/01/26. Complaint Against Police: Stock lane.
20/01/26. RTC: A531 Weston, no injuries.
20/01/26. Highway Disruption: Cobbs Lane Hough, tree in the road.
20/01/26. Domestic Incident: Weston.
20/01/26. Violence/Harassment: Wrinehill Road Blackenhall, relates to a civil dispute.
21/01/26. Highway Disruption: London Road Walgherton, reports of a cow in the road.
22/01/26. Complaint Against Police: Blackenhall.
24/01/26. ASB; Tamwell Road Shavington Park, children causing problems on a building site.
26/01/26. Concern For Safety: Dagfields Crewe Road, note found in a book possibly related to child trafficking in Leicestershire.
27/01/26. Highway Disruption: London Road Bridgemere, tree in the road.
28/01/26. Highway Disruption: Stock Lane Wybunbury, horse reported in the road.
29/01/26. RTC with Injury: Crewe Road Walgherton, male has come off a motorcycle.
29/01/26. Highway Disruption: London Road Stapeley, sheep on the road.
30/01/26. RTC Damage Only: Main Road Wybunbury, slight damage to 2 vehicles.
31/01/26. Hoax Calls to the emergency services: Wybunbury.

WESTON AND CREWE GREEN PARISH COUNCIL

MEETING: 12 FEBRUARY 2026

ASSERTION 10

As part of the Audit requirements for 2025/26, Councils must consider whether they are compliant with Assertion 10, which is as follows (extracts from the 'Practitioners Guide 2025 – Governance and Accountability for Smaller Authorities in England' which is produced by the Smaller Authorities Proper Practices Panel in conjunction with NALC and SLCC.

To warrant a positive response to this assertion, the authority needs to have taken the following actions:

1.1 Email management - Every authority must have a generic email account hosted on an authority owned domain, for example clerk@abcparishcouncil.gov.uk or clerk@abcparishcouncil.org.uk rather than abcparishclerk@gmail.com or abcparishclerk@outlook.com for example.

1.2 All smaller authorities (excluding parish meetings) must meet legal requirements for all existing websites regardless of what domain is being used.

1.3 All websites must meet the Web Content Accessibility Guidelines 2.2 AA and the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 (where applicable).

1.4 All websites must include published documentation as specified in the Freedom of Information Act 2000 and the Transparency code for smaller authorities (where applicable).

1.5 All smaller authorities, including parish meetings, must follow both the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act (DPA) 2018.

1.6 All smaller authorities, including parish meetings, must process personal data with care and in line with the principles of data protection.

1.7 The DPA 2018 supplements the GDPR and classifies an authority as both a Data Controller and a Data Processor.

1.8 All smaller authorities (excluding parish meetings) must also have an IT policy. This explains how everyone - clerks, members and other staff - should conduct authority business in a secure and legal way when using IT equipment and software. This relates to the use of authority-owned and personal equipment.

AGS Assertion 10 — Digital and data compliance

5.1. Data protection and security - Using authority-owned email accounts ensures that sensitive information is handled in a controlled environment with appropriate security measures. This aligns with GDPR principles such as data minimisation, integrity and confidentiality.

5.2. Accountability and transparency - authority-owned email accounts provide a clear record of communications, which is essential for transparency and accountability. This helps in maintaining an audit trail and ensures all authority-related communications are accessible for review if needed.

5.3. Consistency, trust and professionalism - it is best practice to use .gov.uk domains for smaller authorities' emails and websites (excluding parish meetings). This helps maintain a consistent and professional image for the authority and ensures all communications are easily identifiable as coming from the authority. This is increasingly important as cyber scams are on the rise. For support on setting up a gov.uk domain for your smaller authority you can follow the guidance on moving your parish council to a .gov.uk domain.

5.4. Having authority-owned email accounts also makes Data Subject Access and Freedom of Information Requests easier to manage.

5.5. Compliance with policies - All authorities should have an IT policy that mandates the use of authority-owned email accounts for official business. These policies are designed to ensure that all communications are conducted in a manner that is consistent with the authority's standards and legal obligations

5.6. IT Policies - An IT policy prevents misunderstandings when using IT equipment for authority business and makes sure that there can be no excuses for anyone in your authority not protecting their data or working safely. If your authority does not have a policy, you might like to use this IT policy template. It is important to personalise the template for the specific use of your authority and add links to guidance where needed.

5.7. Website accessibility - Where a smaller authority is subject to the requirements of website accessibility it does not have to buy a new website to comply with accessibility law if it places a disproportionate burden on the authority. At a minimum all authorities' websites must include an accessibility statement on their website and keep it under regular review. This statement should include reasons for not meeting accessibility requirements, ways to source alternative copies of non-accessible documents and a point of contact.

5.8. Data Protection - To ensure compliance with data protection regulations, smaller authorities must:

- Appoint a Data Protection officer to oversee data protection and ensure compliance with GDPR.
- Conduct regular data audits to identify what personal data is held, how it is used and make sure it is processed lawfully.
- Implement a Data Protection policy on data handling, storage and sharing.
- Provide regular training to ensure all staff and members are trained on data protection principles and practices.
- Secure data using appropriate technical and organisational measures to protect personal data from breaches.

5.9. The Freedom of Information Act places a duty on every public authority to adopt and maintain a publication scheme which details the publication of information by the authority and is approved by the Information Commissioner; adoption of the Information Commissioners Office model publication scheme meets this requirement.

5.10. In addition to this the Transparency Code for Smaller Authorities requires parish councils, internal drainage boards, charter trustees and port health authorities with an annual turnover not exceeding £25,000 to publish certain information set out in the code. This enables local electors and local taxpayers to access relevant information about the authority's accounts and governance.

5.11. Smaller Authorities with total turnover or expenditure greater than £25,000 should as best practice comply with the Local Government Transparency Code 2015; the government believes that in principle all data held and managed by local authorities should be made available to the public unless there are specific sensitivities to doing so.

5.12. Monitoring an authority's compliance with the relevant transparency code is not part of the external auditor's limited assurance review of the AGAR. It would however be expected that internal auditors would review this control area.

Commentary:

The Council is in a good position regarding adherence to this assertion, having already adopted a .gov.uk website domain name and official Councillor email addresses utilising the Council's official address. The Council has been compliant with all of the data protection and accessibility legislation as it has been implemented.

However, this is an opportune time to review all policies and procedures to ensure continued compliance and ensure continued adoption of best practice.

The following are the actions the Clerk will undertake before the end of the financial year:

Email management	No action required
Website compliance with WCAG 2.2	To check compliance and make any adjustments necessary.
Website contains all necessary documentation	No action required (noting that the Transparency Code does not apply to the Council)
Data Protection and GDPR	Review the Data Protection Roadmap (undertaken previously but opportune to review)
IT Policy	A number of policies already exist but to agree an overarching policy

WESTON AND CREWE GREEN PARISH COUNCIL

INFORMATION TECHNOLOGY POLICY

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

1.1 Hardware

1.1.1 council computer equipment is provided for council purposes only.

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

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

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

1.1.5 All computer and mobile equipment will be logged on the Council' Asset Register.

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

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

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 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).

2.2 Use of own devices

2.2.1 Wherever possible Councillors 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.

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

2.2.3 Personal data relating to Councillors, staff, and other authorised users, associates, residents, external stakeholders should not be saved to any personal accounts with third-party storage cloud service 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.

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

2.2.5 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.

2.2.6 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 Chair or other nominated Councillor to access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.7 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 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

3.1.2 Any VDU user who feels that their workstation requires changes to make it compliant must speak to Chairman

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

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 Council
- 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 Chairman 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.

Monitoring

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

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

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

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

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

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

5.1.10 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to

retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

5.1.11 The council 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.

5.1.12 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 or at meeting venues:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the devise does not clearly support these actions (for example at an internet café), council services should not be accessed from that device;
- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc;
- any data printed should be collected and stored securely;
- all electronic files should be password protected and the data saved to the council's system/services when accessible;
- 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 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 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 external stakeholders 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.

9.1.3 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:

- 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 its current or potential 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.
- 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 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

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.