



Dartmoor Forest Parish Council

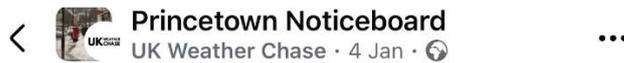
20th February 2025

Councillor Briefing Notes for Council Meeting on 24th February 2027 7.30 pm in Princetown Community Centre

1. **Apologies** –
2. **Declarations of interest** –
3. **Urgent decisions since last meeting** –
4. **Acceptance of minutes** - As previously circulated for meeting on 27th January 2025.
5. **Updates from Devon County Councillor and West Devon Borough Councillor** – if in attendance.
6. **Princetown ward vacancy** – Council to discuss and agree recruitment plan to co-opt at March meeting.
7. **Additional Defib for Princetown** – As raised at January meeting - Council to consider and agree whether additional Defib for Princetown is necessary, and discuss possible funding options. See Appendix 1 for cost of defib to match others within Parish and outdoor cabinet (required to keep defib at correct working temperature if sited outdoors).
8. **Phone Box, Woodville** – Council to discuss and agree on how box can be used in the future.
9. **Local Government Reorganisation - Consultation** – Council to consider and agree whether to respond to consultation. (deadline 26th March 2026) See email circulated to all Cllrs on 11/02/26 <https://www.devonlgr.co.uk/>
10. **Residents' issues or concerns** – Updates on issues raised at January meeting. Council to consider and agree on any further action to be taken.
 - a) Request for additional grit bin at the bottom of Burrator Avenue, Princetown. Unfortunately, no funding is available from DevonCC Localities budget for a replacement bin. Council to consider approaching other funding sources to raise the £350 necessary eg. Princetown Charity Shop, or agree to fund from Council reserves
 - b) Dog mess in Jubilee Field, Princetown as agreed at last meeting Clerk investigated cost of additional 'Clean up after your dog' signs see Appendix 2
11. **1st PUBLIC SESSION** - Residents are invited to give their views and question the Parish Council on agenda items or raise issues for future consideration.
12. **Planning** – Council to consider, discuss and agree on response regarding the applications listed below as emailed to Cllrs on 12/12/26
 - a) [048/25](#) Brimpts Farm, Dartmeet, PL20 6SG deadline 03/03/26
13. **Request for funding from Crimestoppers South West Region** - Council to consider and agree on whether to make a donation as emailed to all Cllrs on 11/02/26, [DFPC Grants and Donations Procedure](#) has been emailed to Crimestoppers. See Appendix 3 for donation request for £75 received 16/02/26
14. **Financial management** - see Financial Report for details
 - a) Payments to be approved

15. Updates on correspondence/ actions from previous meetings

- a) Parish Calendar 2026 – update on refund and replacements.
- b) Bin replacement/repair Princetown – update from WDBC
- c) Princetown Community Centre – update on meeting 31st Jan 2026
- d) Phone Box Memorial – update on relocation of information
- e) Snow and Ice events -
 - update from correspondence with UK Weather Chaser and Plume of Feathers and Council to agree on any further action to be taken.
See email from Cllr Grover 15/02/26



Please stay weather aware and use the brain before heading out. 😊

UK Weather Chase 4 Jan · 🌐

With snow forecasted, can we politely ask everyone to be weather-prepared.

We all love a snowy day, sledging, snowmen, "just a quick drive out to see what it's like"... but let's not forget what happened last year. It was horrendous on [#Dartmoor](#), Cars abandoned on roadsides, traffic at a standstill, and multiple families, including kids stuck for hours in freezing conditions.

Snow can turn from magical to miserable very quickly, especially when children are involved. Being unprepared can turn a great day out into a complete disaster faster than you can say "we'll be fine."

Not teaching you how to suck eggs but put your brain into gear before jumping in the car.

So before heading out, just think first:

- Check the forecast and road conditions
- Pack essentials (warm clothes, blankets, food, water, phone charger)
- Make sure your vehicle is winter-ready
- Have a recovery plan in case you do get stuck

Enjoy the snow, laugh at the chaos, take the photos, but stay alert and prepared. A little planning now can save a lot of stress later. Stay safe out there 🧑‍🚒 🚗

Lastly, if around Princetown, check in [Plume of Feathers Princetown](#), there hot chocolates are insane! 😍 [#WeatherAware](#) [#UKSnow](#)

- report from Cllr Mark Williams regarding locking of Car Park and Council to agree any further action to be taken.
- f) Thankyou letter to Catherine and Roger Charlton - council to agree to send draft as written by Cllr Geen. (emailed to all Councillors on 15/02/26)

16. Reports and Updates from Committees, Sub Groups and Special Interests

- a) CCTV System Check & any requests – CCTV Working Group –

01/02 HW questioned if 'events' were being recorded, 01/02 JB – Checked events are being recorded, 15/02 LE - all OK

- b) Sensory Garden – Meeting with Emma Morrison, Hazel Williams, Jackie Bennetts and Duncan Clerk planned for 03/03. Start date for project 1st May 2026.
- c) Playpark – Inspections and Litter picking see Appendix 4 for action plan.
- d) LOVE (Love Our Village Enthusiasts) Project –
- e) Tidy Princetown Sessions –
- f) Defib Checks –
- g) Speedwatch – Group is unable to receive the funds held by DFPC as they have no bank account. Council to discuss with them how they wish to spend the remaining £1320.26 asap, or ask if they would consider officially donating the funds to DFPC for it to spend on road safety issues.
- h) Gardening the Grounds -

17. 2nd PUBLIC SESSION - Residents are invited to give their views and question the Parish Council on agenda items, or raise issues for future consideration

18. Exchange of information – Around the table discussion for any matters to be shared for information or to request they are put on agenda for next meeting:

- a) **DFPC Policy Review** - see Appendix 5 for policies in need of review in coming months.
- b) **Assertion 10** - DALC webinar 4th March 2026
<https://devonalc.org.uk/events/demystify-assertion-10/>
- c) **Assertion 10** - Implications for DFPC – IT Policy, see Appendix 6 for NALC template.
- d) **Jubilee Field ownership**
- e) **North Bovey Parish Beating the Bounds** - 2nd or 4th May, to be confirmed.
- f) **0064/26 Planning Application** - re Dartmoor Brewery Ltd Station, received 19th February with 21-day response period.

19. Date of next meeting -

Council Meeting

1930 on Tuesday 24th March 2026
Princetown Community Centre

Appendix 1

<https://defibwarehouse.co.uk/shop/defibrillators/zoll-aed-plus-fully-auto/?>

ZOLL AED Plus Fully Automatic Defibrillator



£875.00 (excl.VAT)

£1 050,00 (incl.VAT)

In stock

Extra options to add

Defibrillator Product Support and 4 hour AED Training Course options are available for every Live AED and Defibrillator Package purchase.

Our AED Service/Health Check is available for new and existing customers.

- Defibrillator Product Support (+£99.00)
- 4 hour AED Training Course (+£595.00)
- AED Service/Health Check (+£200.00)
- Wall Signs & Rescue Kit Bundle (+£29.99)

1

Add to basket

<https://defibwarehouse.co.uk/shop/cabinets-brackets/aivia-200/?>

AIVIA 200 Outdoor AED Cabinet



£450.00 (excl.VAT)

£540,00 (incl.VAT)

In stock

1

Add to basket

Pay in 3 interest-free payments of £180.00 with [PayPal](#) [Learn more](#)

The AIVIA 200 alarmed AED cabinet can be installed indoors or outdoors. This strong and durable AED cabinet is alarmed and heated to give your AED maximum protection from the elements if stored outdoors. This is a very popular product and one of our best sellers!

<https://defibwarehouse.co.uk/shop/cabinets-brackets/aivia-210-aed-cabinet/?>

AIVIA 210 Outdoor AED Cabinet With Lock



£465.00 (excl.VAT)

£558,00 (incl.VAT)

In stock

1

Add to basket

Pay in 3 interest-free payments of £186.00 with [PayPal](#) [Learn more](#)

The AIVIA 210 Outdoor AED cabinet has been designed for outdoor installation. This strong and durable AED cabinet is alarmed, heated and keycode accessible to give your Defibrillator maximum protection from the elements when stored outdoors.

Appendix 2

<https://www.thesignshed.co.uk/>

CART 4



Clean Up After Dog Sign
300 x 400 mm, 1mm Rigid Plastic, Holes in 4 corners
£9.50 (inc. VAT) ~~£11.50~~ (inc. VAT)

- 1 +

£9.50
(inc. VAT)



Clean Up After Dog Sign
300 x 400 mm, 3mm Recycled Plastic, Holes in 4 corners
£15.50 (inc. VAT) ~~£19.50~~ (inc. VAT)

- 1 +

£15.50
(inc. VAT)



Clean Up After Dog Sign
A4 (210 x 297 mm), 1mm Rigid Plastic, Holes in 4 corners
£7.50 (inc. VAT) ~~£9.50~~ (inc. VAT)

- 1 +

£7.50
(inc. VAT)



Clean Up After Dog Sign
A4 (210 x 297 mm), 3mm Recycled Plastic, Holes in 4 corners
£9.50 (inc. VAT) ~~£11.50~~ (inc. VAT)

- 1 +

£9.50
(inc. VAT)

Appendix 3 received by email 16/02/26

Name of organisation; Crimestoppers South West Region

Contact ; Karen MacDonald Regional Manager for the South West

Crimestoppers Trust, registered charity in England & Wales (1108687), Scotland (SC037960). A company limited by guarantee, registered in England and Wales No. 05382856. Registered address: Sedulo London, Office 605, Albert House, 256-260 Old Street, London EC1V 9DD. Postal address: Crimestoppers Trust, PO Box 324, Wallington SM6 6BG.

email karen.macdonald@crimestoppers-uk.org **phone;** 07917793636

website www.crimestoppers-uk.org

facebook profile www.facebook.com/CrimestoppersintheWestCountry

Amount applied for ;£75

Purpose of grant; Increase reporting of crime, improve public confidence to report and increase community safety.

What will the money help you achieve; Raise awareness of our independent charity. We are the only crime fighting charity offering anonymous reporting through our free number 0800 555 111 or our website www.crimestoppers-uk.org

What will you spend the money on; Digital, social and print media within your parish plus presentation to a parish meeting explaining our call to action which is to speak up, stop crime and stay safe whilst remaining 100% anonymous. Always. Examples of resources attached = generic piece for the parish council website, example of a generic social media asset and an example of a leaflet (drink/drug drive)

Anticipated benefit to the Parish; Increase reporting of crime, improve public confidence to report, decrease crime and improve cohesion in your community.

What resources are being contributed - Project management, volunteer time and presentation to parish council and registration into our Ambassador programme [Community Ambassadors | Crimestoppers](#)

Thankyou for your attention.

best regards

Karen

Karen MacDonald

Regional Manager South West

Crimestoppers Trust, PO Box 324, Wallington, SM6 6BG
Mobile:[07917 793636](tel:07917793636), Email:Karen.MacDonald@crimestoppers-uk.org
Website:www.crimestoppers-uk.org | Switchboard:020 8835 3700

Appendix 4

Dartmoor Forest Parish Council Governance Documents, Policies, Procedures and Risk Assessments						
	Governance Docs	Policy	Procedure	Assessment	Notices	
	Documents	Date of last Review	Review Frequency	Review Due	Notes	Suggested Lead Reviewers At least two councillors needed to review each
0	Risk Register	Jul-25	3 monthly	Jul-26		All relevant
0	Risk Management Strategy	Apr-24	2 years	Jun-26		Clerk, Cllrs Geen & H Williams
1	Standing Orders	Apr-24	Annual	Apr-26		Clerk & All Councillors
2	Financial Regulations	Nov-25	Annual	Nov-26		Clerk, Cllrs Geen & M Williams
2.1	Grants and Donations Procedure	May-24	2 years	Aug-26		Cllrs Geen &
3	Members' Code of Conduct	May-24	Annual	Jul-26		All
3.1	Complaints Procedure	May-24	2 years	Aug-26		Cllr Watson and Cllr H Williams
4	Transparency Code	May-24	Annual	Jul-26		All
4.1	Community Engagement Policy	Feb-25	2 years	Feb-27		Cllr Easton & Cllr H Williams
4.1.1	Publication Scheme	Oct-24	2 years	Sep-26		Clerk
4.1.2	Privacy Notice	Oct-24	2 years	Sep-26		Clerk
4.2	Princetown CCTV Policy	Dec-24	Annual	Apr-26		CCTV Working Group Chair & Vice & Cllrs H Williams & Edis
4.2.1	Princetown CCTV Data Protection Impact Assessment	Dec-24	Annual	Apr-26		CCTV Working Group Chair & Vice & Cllrs H Williams & Edis
4.3	Safeguarding Policy	Feb-25	2 years	Feb-27		
4.4	Equality Diversity & Inclusion Policy	Oct-25	2 years	Oct-27		
4.5	Whistleblowing policy	Nov-25	2 years	Nov-27		
5.1	Play Area Inspections Procedure	Feb-25	Annual	Feb-26		Cllrs M Williams & Grover
5.2	Lengthsman and Grounds Maintenance Procedure	May-25	Annual	May-26		Clerk & Cllr M Williams
5.2.1	Lengthsman and Grounds Maintenance Risk Assessment	May-25	Annual	May-26		Clerk & Cllr M Williams
5.3	Snow Warden Procedure	Mar-24	2 years	Mar-26		Cllr Easton
5.3.1	Snow Warden Risk Assessment	Mar-24	2 years	March 2026		Cllr Easton
5.4	Memorial Inspections Procedure	Mar-24	2 years	Mar-26		Clerk, Cllrs Watson & Smerdon
5.5	Postbridge Cemetery Burials (current)					
5.5	Postbridge Cemetery Plots and Burials from 1.4.2026	Nov-25	2 years	Nov-27		Clerk, All
5.6	Public Seating	Oct-25	2 years	Oct-27		Cllrs Cotterill & Edis
	Climate Declaration	? Before 2022				

Appendix 5 - RoSPA Play Park Inspection March 2025 – Action Plan -

Element	What	Who	Notes / Completed
P1 - Agility Trail	Edges of new timber need to be radiused (3mm) or chamfered (3mm). Chain Link connectors notched – to be replaced Timber decayed – to be monitored	DC	Edges rounded
P3 – Cableway	Remove chain cover to inspect chain links to seat	DC	
P9 – Rocking Horse	De-scale back to good base material and coat with lead free paint. Repairs may be necessary where corrosion is severe Matting has shrunk back badly and needs lifting, surfaces cleaning and mats re-stuck.	DC DC	Rubbed down Adhesive ordered 08/25
P11 - Seesaw	Repair – wear to internal mechanism resulting in excessive sideways movement - <i>25/01/25 Bearing & Seats replaced</i> De-scale back to good base material and coat with lead free paint. Repairs may be necessary where corrosion is severe	DC DC	Bushes ordered 17/6 & Fitted 19/08 Autumn 2025
P15 – Mixed Swings	Remove shackle bolt and check bushes and shackle pin wear – replacing as necessary Chain Links notched – replace as necessary	DC DC	
P16 – Swing – single point	Surface is uneven – make good small area where edge of matting is exposed and lifting (trip hazard)	DC	
Fencing – boundary with PCC bank/car park	Several posts are not secure (rotten at ground level) Top rail is missing in places and split in others Middle rail is also split in places Option A: To replace entire length of fence – 32x 4x4inch posts (5'6") and 16 12' rails 3.5"x1.5" plus stock netting Option B: Alternative measure could be to put new posts between existing posts and replace rails as necessary. 10 posts and 5 rails as above. Plus labour costs. DC to quote for time taken to make full repair. At least two additional quotes to be obtained for comparison.		On hold due to responsibility for fence lying with PCC

Appendix 6 – NALC template IT policy

[ENTER COUNCIL NAME] INFORMATION TECHNOLOGY POLICY

Introduction	ERROR! BOOKMARK NOT DEFINED.
Purpose of the IT Policy	10
Monitoring of IT use	10
Scope of this policy	10
Computer use	10
Equipment	11
Health and safety	15
Password and authentication policy	15
Monitoring	16
Remote working	18
Email	ERROR! BOOKMARK NOT DEFINED.
Use of the internet	19
Use of social media	20

Introduction

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

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

Purpose of the IT Policy

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

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

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

Monitoring of IT Use

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

Scope of this policy

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

Computer use

Hardware

[Either] council computer equipment is provided for council purposes only. [or] Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of [specify whom, e.g. "the council,

1.1.1 [the clerk"]. Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

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

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

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

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

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

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

1.1.8 Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of [specify whom, e.g. the council].

1.1.9 [Delete if not appropriate] The council has a number of wireless networks. Using a portable device to make personal Wi-Fi hot spots which bypass existing WiFi is not allowed.

1.1.10 [Optional] Any faults or necessary repairs must be reported to [specify whom, e.g. "the clerk/ IT provider"].

Equipment

2.1 Portable equipment

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

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

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

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

2.1.5 [Optional] 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 [specify whom, e.g. “the clerk/IT provider”]. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first [specify amount] of the loss/damage.

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

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

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

2.2 Use of own devices

[Choose either “no use permitted” below and delete the whole of the rest of this section, or “some use permitted” and tailor to suit.]

2.2.1 Personal laptops and other computers or other devices should not be brought into work and used to access council IT systems during working hours, unless this has been authorised by the employee’s line manager. This is to ensure that no viruses enter the system, to prevent time being wasted during working hours on personal use and to assist in maintaining security, confidentiality, and data protection.

[or – if some use is permitted – delete the above, and tailor the remainder of this section, including the options regarding data storage below.]

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

2.2.3 However, the same security precautions apply to personal devices as to the council's desktop equipment. For continuity purposes, calls made to external parties (such as [specify, e.g. "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.

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

2.2.5 In cases of legal proceedings against the council or [specify, e.g. "external stakeholders"], the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

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

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

- use a [specify, e.g. "6-digit pin, strong password (i.e. one which uses three random words (e.g. PurpleCandleRiver) or finger print (preferably the latter)"] to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after [specify number] of failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than [specify duration];

- 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 [specify whom, e.g. "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.

[Tailor either this section or the alternative section below, as appropriate:]

2.2.8 Personal data relating to [specify, e.g. "councillors, staff, and other authorised users, associates, residents, external stakeholders"] should not be saved to any personal accounts with third-party storage cloud service providers (e.g. [specify name of service provider]) as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

2.2.9 Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time. The following data must never be accessed or processed on a personal device: [specify device].

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

2.2.11 Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use. [Specify job title or department] will provide assistance or training in doing this if needed. Additional risks include data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

2.2.12 [or – if work is allowed to be saved onto personal equipment:> <Optional – tailor to suit:] Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

2.2.13 [Optional]. If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used.

2.2.14 Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to allow [specify whom, e.g. "the IT provider"] access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

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

Health and safety

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

3.1.2 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in the council's [specify, e.g. "display screen equipment policy" or "health and safety policy"].

3.1.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to [specify, e.g. "the clerk"].

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to [specify job title e.g. "councillor/ clerk" or "the IT provider"].

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 [specify e.g. chair of council], in a sealed envelope, only to be accessed in an emergency.

4.1.3 Password Storage and Management

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

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

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

4.1.6 Responsibility

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

The IT security provider is responsible for:

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

Monitoring

5.1.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to

ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

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

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

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

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

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

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

5.1.11 The council has software and systems in place that can [optional: "prevent inappropriate internet use and"] monitor and record all internet usage. A daily log is kept of all activity, which details the names of all websites accessed, along with the date and time of access, by individual councillors, staff, and other authorised users. Records of internet use and sites visited will normally be retained for a period of [specify duration, e.g. "six months"].

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

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

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

Remote working

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

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the 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 a [specify, e.g. "non council"] premises unless arrangements have been made with a responsible person at a [specify, e.g. "non council"] premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time;
- any data should be kept safely and should only be disposed of securely;
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed;
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft;
- Councillors, staff, and other authorised users who work away from the office with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

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

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

7 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.

7.1.1 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.

7.1.2 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 [specify, e.g. "IT provider"], rather than assuming they know the right answer.

7.1.3 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.

7.1.4 [Either] Email messages sent on the council's account are for council use only. Personal use is not permitted.

[or] Email messages sent on the council's account should be for council use only. Personal communications are permitted provided they do not encroach upon working time or interrupt council business in any way. Employees and other authorised users are asked to restrict their personal use to official lunch breaks or before or after working hours, and to use their personal email accounts, rather than council addresses.

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 [specify, e.g. “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 [specify, e.g. “the council/ 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 [specify location, e.g. “included in the Employee Handbook”].

8.3 Accuracy of information

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

Use of social media

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

9.1.2 Personal use of social networking/media and chat sites [choose either] are not permitted during working hours [or] should be restricted to breaks during working hours, or after hours with permission.

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

However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks 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.

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

[Tailor the following list to suit]

- 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 [specify, e.g. "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, [specify e.g. "our current or potential plans, councillors, staff, and other authorised users, partners"], must inform [specify whom, e.g. "the clerk/ the council"] that they are writing this and gain agreement before going 'live'.
- The council expects councillors, staff, and other authorised users to be respectful about the council and its current or potential <[specify e.g. "all staff, including employees, councillors, clerks, and authorised users"] and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.
- Photos or videos that include employees or other workers wearing uniforms or clothing displaying the council's name or logo should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues, or the council. Additionally, photos, videos, or audio recordings must not be taken on council premises without explicit permission
- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations with [specify whom e.g. "external stakeholders"] should not take place on any social networking sites, including forums.

Any writing about or displaying photos or videos of internal activities that involves current councillors, staff, and other authorised persons, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their

permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff, and other authorised users anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.

- Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other councillors, staff, and other authorised users can raise grievances for alleged bullying and/or harassment.
- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council or its [specify e.g. "councillors, staff, and other authorised users"], 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 [specify whom e.g. "the clerk"].
- Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors, staff, and other authorised users who use X.com, LinkedIn, or other social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff, and other authorised users on LinkedIn, Facebook, X.com or any other social media/networking sites.
- During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor, member of staff, or other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

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

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

Misuse

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

Guidance

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

Important notice

This is an example of a policy designed for a small council adhering to statutory minimum requirements and does not constitute legal advice. As with all policies it should be consistent with your terms and conditions of employment.

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

This document has been written by Worknest HR – a company that provides HR advice and guidance to town and parish Councils. Please contact them on 01403 240 205 for information about their services.