



Appendix A

FRATING PARISH COUNCIL

Memorial Hall, Main Road, Frating, CO7 7DJ.

Clerk to the Council: Kay English

Email: clerk@fratingparishcouncil.gov.uk

Website: www.fratingparishcouncil.gov.uk

MINUTES of the FRATING PARISH COUNCIL MEETING held at the Memorial Hall on Monday 3rd November 2025 at 19:30hrs.

Present: Cllr Terry Cuthbert (Chairman)
Cllr Paula Bland (Vice Chairman)
Cllr Jean Hynes
Cllr Sally Potter
Kay English, Clerk to the Council
There was one member of the public.

Chairman's Announcement

Cllr Cuthbert notified the Council of Terri Philp's resignation from office. The Council expressed its gratitude to Mrs Philp for her service and dedication to Frating Parish Council (FPC) throughout her term. It was further acknowledged that two councillor seats were now vacant.

11.25.81 APOLOGIES FOR ABSENCE

Apologies for absence were RECEIVED and ACCEPTED from Cllr Veronica Morris

11.25.82 DISCLOSURE OF INTERESTS

It was **RESOLVED**: That members would raise relevant disclosures of interest at applicable agenda item.

11.25.83 PUBLIC QUESTIONS

Question 1: An enquiry was received regarding the hoarding and associated works on Haggars Lane.
Response:

The planning application was reviewed; Tendring District Council confirmed that the hoarding met safety standards. FPC had no further authority to accelerate the progress of the works.

Question 2:

A noticeable reduction in surface water was observed following a recent period of heavy rainfall.

Response:

Essex County Council Highways carried out drainage and ditch clearance, which helped alleviate the issue. FPC had actively collaborated with relevant agencies and was currently awaiting an update on the latest developments.

Statement:

FPC was informed that the Great Bentley Carnival was unlikely to proceed next year.

11.25.84 MINUTES

Members RECEIVED and CONSIDERED the draft Minutes of the Frating Parish Council (FPC) meeting held on 6th October 2025 (Appendix A)

It was RESOLVED: That the Minutes of the meeting held on Monday 6th October 2025 be APPROVED and signed by the Chairman.

11.25.85 MATTERS PENDING

Members RECEIVED and CONSIDERED a list of the Parish Council's current outstanding actions as outlined in Appendix B. An update on some of the outstanding matters was given:

- i. Vehicle Speeding: The Essex Highways Department's traffic survey report was recently requested.
- ii. Lukins Farm Planning: Developer contributions for traffic light improvements were noted as insufficient; Cllr Guglielmi would be asked for further clarification on this, particularly regarding the LHP disbandment.
- iii. New Mineral Site: Increased lorry movements were expected once work begins.
- iv. Transfer of Churchyard: A meeting was scheduled to finalise works such as rubbish clearance, after which funds from TDC would be released. Risk assessments on gravestones and possible repositioning of iron works was needed. Additional requirements included signage and research on the Commonwealth grave's history.

It was RESOLVED: That Matters Pending be NOTED

11.25.86 REPRESENTATIVES' REPORTS

- i. Cllr Carlo Guglielmi (ECC) gave his apologies; his report was circulated by email prior to the meeting.
- ii. Cllr Aimee Keteca (TDC) gave her apologies.
- iii. There were no FPC representative reports.

Response: that the report received from Cllr Guglielmi be NOTED.

11.25.87 CHAIRPERSON'S REPORT

- i. Surface Water Flooding (MAG10):

A meeting was held with the relevant agencies, and progress was noted. Anglian Water would be requested to provide further details on their investigations, especially with winter approaching. A follow-up meeting was scheduled for December.

- ii. Public Rights of Way (P3) Signage:

Wayfinding signage had been ordered but not yet delivered.

- iii. Fraud Awareness:

The Chairman attended a fraud awareness presentation delivered by Essex Police at Lawford Parish Council's new premises.

- iv. Frating Heritage Pump:

No further updates were available at this time.

- v. Bins:

Litter and dog waste bins have been ordered, with delivery expected within 4–6 weeks.

It was RESOLVED: That the Chairman's report be NOTED and that the Clerk requests a Fraud Awareness presentation to be given at the Annual Parish Meeting.

11.25.88 CLERK'S REPORT

The Clerk:

- i Logged a total of 24 working hours in September 2025.

- ii Enrolled to attend the Budget & Precept course and the Law & Procedure course in November 2025, as part of her continued professional development.

It was RESOLVED: That the Clerk's report be NOTED.

11.25.89 PLANNING & ENVIRONMENT

- i. Planning Applications:

25/01558/FULHH: planning application for single and two-storey rear extension, single storey front port, new render cladding and installation of PV panels to roof: 1 Council Houses, Bromley Road

It was RESOLVED: that there were no comments or objections.

- ii. Planning Determinations:

25/01224/NDPN: planning application for roof mounted solar PV arrange on non-domestic building premises: Manheim Colchester Auctions in Great Bentley

It was RESOLVED: that the Planning decision be noted.

- iii. Planning Appeals:

None were received.

- iv. Vehicle-Activated Sign report (Appendix C): it was noted that there was around 6% of vehicles exceeding the speed limit entering the village and 13% exiting the village.

It was RESOLVED: that the number of speeding vehicles be kept under review.

11.25.90 FINANCE

i. Electricity Supply – Npower: The Clerk reported that a refund of £1,254 was due from the previous street lighting electricity supplier, Npower. The FPC account was adjusted as part of Npower's nationwide transition for unmetered supplies, which involved revising procedures for collecting and settling consumption data.

It was RESOLVED: that the credit from NPower be noted.

ii. EALC Community Grants: up to £10,000 was available for Town & Parish Councils' projects as outlined in Appendix D, with applications due by 28th November 2025. The Memorial Hall Management Committee would be applying for a grant for window replacement. FPC would consider support for other potential work, such as floor revarnishing, at a future meeting.

It was RESOLVED: that the availability of the EALC community grant be noted and that an application for window replacement would be submitted by the Memorial Hall Management Committee.

iii. FPC Budget 2026/27: The proposed budget for financial year 2026/27 as outlined in Appendix E was considered.

It was RESOLVED: that the budget as presented in Appendix E be APPROVED and in line with this, the Precept for 2026/27 of £16,326 was also APPROVED.

iv. Schedule of Payments and Receipts 01.10.25 – 31.10.25 (Appendix F)

It was RESOLVED: that the schedule of payments and receipts be APPROVED.

v. Schedule of Invoices presented by the Clerk (circulated prior to the meeting)

It was RESOLVED: that the schedule of invoices as presented by the Clerk be APPROVED.

11.25.91 COMMUNITY & LEISURE

i. Litter Pick:

It was RESOLVED. That a litter pick would take place on 29th November 2025.

ii. Churchyard Open Spaces: this was addressed in minute 11.25.85 Matters Pending.

11.25.92 ITEMS FOR INCLUSION ON THE AGENDA OF A FUTURE PARISH COUNCIL MEETING

Items for inclusion on the agenda for the next meeting should be referred to the Clerk.

Under this the failing manhole cover on footpath was noted, which the Chairman would report.

11.25.93 DATE OF THE NEXT PARISH COUNCIL MEETING

The next Parish Council meeting was scheduled to take place on Monday 1st December 2025 at 19:30hrs at Frating Memorial Hall.

The meeting closed 20:30 hours.

Signed..... Date.....



Appendix B

FRATING PARISH COUNCIL

Memorial Hall, Main Road, Frating, CO7 7DJ.

Clerk to the Council: Kay English

Email: clerk@fratingparishcouncil.gov.uk

Website: www.fratingparishcouncil.gov.uk

AGENDA ITEM 5 – MATTERS PENDING

PLANNING & ENVIRONMENT

- 04.25.149** i.Road Safety measures: reduction in speed limit to 30mph
ii.New Mineral Site A69.

LEISURE & FACILITIES

- 04.25.45** Transfer of Churchyard.

COMMUNITY

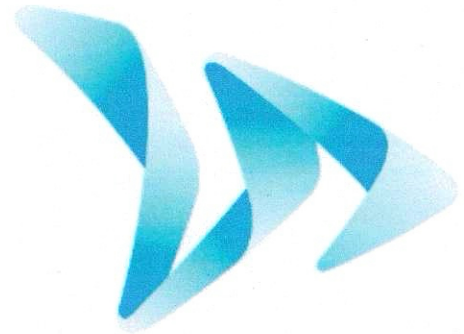
- 05.25.13** Thorrington Church, Frating: support and promotion.

GOVERNANCE

- 06.25.29** S101 Agreement/S106 Funds: Closed Churchyard.

Appendix C

ÉlanCité



DÉTECTER • INFORMER • SÉCURISER

Start date: Thursday, October 23, 2025 12:00 AM
End date: Friday, November 21, 2025 11:00 AM

Location:

Comments:

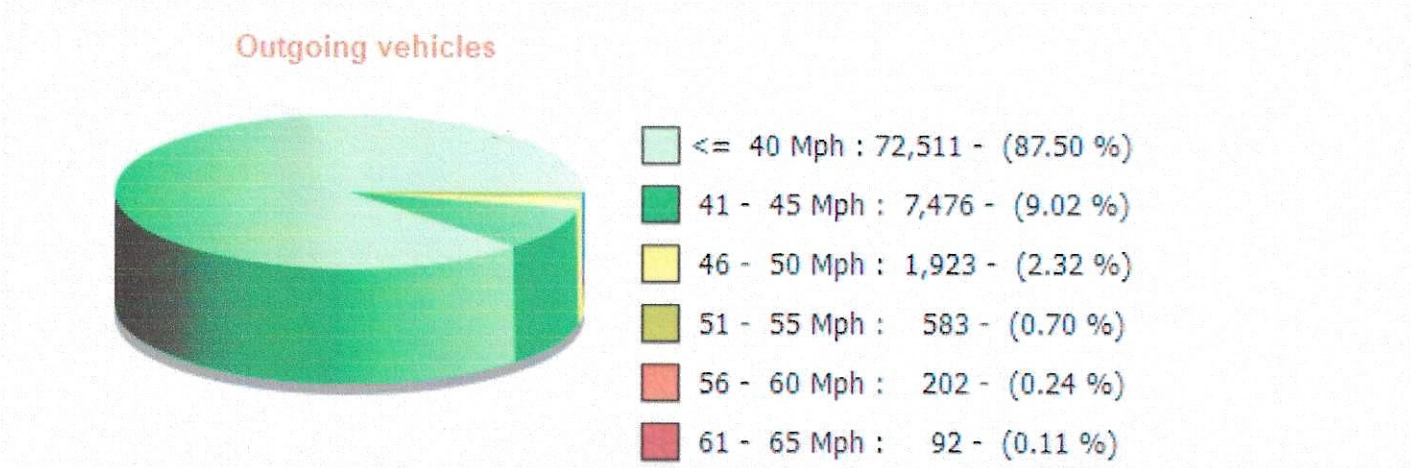
Incoming vehicles



Start date: Thursday, October 23, 2025 12:00 AM
End date: Friday, November 21, 2025 11:00 AM

Location:

Comments:



Start date: Thursday, October 23, 2025 12:00 AM
End date: Friday, November 21, 2025 11:00 AM

Location:

Comments:

Appendix D

Frating Parish Council

PAYMENTS & RECEIPTS LIST

22 November 2025 (2025-2026)

Vouche	Code	Date	Minute	Bank	Cheque No	Description	Supplier	VAT Type	Net	VAT	Total
92	PAYE/NI	03/11/2025		Current Account	Q2 Ending 5/10/2025	Payment - PAYE/NI	HMRC	X	-241.30		-241.30
											-241.30
93	Contract Maintenance	03/11/2025		Current Account	Invoice 3140	Payment - Tree Cutting	Landscape Services	S	-350.00	-70.00	-420.00
											-420.00
94	Training	03/11/2025		Current Account	Invoice 18892	Payment - Training	EALC	S	-84.00	-16.80	-100.80
											-100.80
95	Expenses	03/11/2025		Current Account		Payment - Clerk Expenses	Frating Parish Council	X	-9.38		-9.38
											-9.38
96	Contract Maintenance	03/11/2025		Current Account	Invoice 3141	Payment - Grass Cutting	Landscape Services	S	-125.00	-25.00	-150.00
											-150.00
97	Expenses	03/11/2025		Current Account	Invoice 120023165	Payment - Poppy Wreath	Royal British Legion	S	-24.57	-4.92	-29.49
											-29.49
98	Stationery	03/11/2025		Current Account	202-4711291-2380	Payment - Stationary	Amazon	S	-7.50	-1.50	-9.00
											-9.00
99	Subscriptions	03/11/2025		Current Account		Payment - Adobe Subscription	Adobe Ltd	S	-16.64	-3.33	-19.97
											-19.97
100	Public Lighting	03/11/2025		Current Account	Invoice 3607424	Payment - Electricity	SSE Energy Solutions	S	-137.02	-27.40	-164.42
											-164.42
101	Chairperson's Allowance	03/11/2025		Current Account		Payment - Chairperson's Allowance	Frating Parish Council	X	-34.27		-34.27
											-34.27
102	Clerk Salary	03/11/2025		Current Account		Payment - Clerk Salary	Frating Parish Council	X	-332.50		-332.50
											-332.50
103	Bank Charges	03/11/2025		Current Account		Payment - Bank Service Charge	Unity Trust Bank	X	-6.00		-6.00
											-6.00
Total									-1,368.18	-148.95	-1,517.13



Appendix E

FRATING PARISH COUNCIL

Memorial Hall, Main Road, Frating, CO7 7DJ.

Clerk to the Council: Kay English

Email: clerk@fratingparishcouncil.gov.uk Website:

www.fratingparishcouncil.gov.uk

INFORMATION TECHNOLOGY POLICY

Introduction	2
Purpose of the IT Policy	2
Monitoring of IT use	2
Scope of this policy	2
Computer use	2
Equipment	3
Health and safety	5
Password and authentication policy	5
Monitoring	6
Remote working	7
Email	8
Use of the internet	8
Use of social media	9

Introduction

Frating Parish Council (FPC) values secure, effective IT and email use for its operations. This policy provides guidance on proper IT and email usage for council members and staff.

Purpose of the IT Policy

This IT policy defines how councillors, staff, and authorised users should use council technology and equipment. It aims to:

- Specify proper use of systems;
- Highlight IT risks;
- Protect council data and assets;
- Define acceptable and unacceptable actions;
- State consequences for breaches.

Monitoring of IT Use

FPC may monitor its IT equipment and systems for legitimate reasons, as long as users, including councillors, employees, and others with system access are informed that monitoring may occur. Such monitoring must be proportionate and comply with data protection and privacy laws.

Scope of this policy

The policy applies to all individuals who use FPC IT resources including computers, networks, software, devices data and email accounts 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 FPC computer equipment is provided for council purposes only, however reasonable personal use is permitted as determined by the council. Any personal use of FPC computers and systems should not interrupt daily council work or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights and must not access inappropriate or offensive content.

1.1.2 All councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work purposes.

1.1.3 All computer and electronic equipment provided must be handled with care; devices represent a significant investment and any damage incurred will result in financial consequences for the council.

1.1.4 Councillors, staff, and other authorised users should not purchase any computer or mobile equipment (including software) unless previously authorised.

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

Equipment

2.1 Portable equipment

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

2.1.2 All portable computers must be stored safely and securely when not in use 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 working premises and should never be left in parked vehicles or at any council or non-council premises.

2.1.3 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.

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

2.1.5 To protect confidential information, unless it is a requirement of the job and this has been authorised, photographs or videos must not be taken on council premises, without the prior written permission of the council. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

2.1.6 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).

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

2.2 Use of own devices

2.2.1 Personal laptops and other computers or other devices should not be brought into work and used to access council IT systems during working hours, unless this has been appropriately authorised. This is to minimise the risk of viruses entering the system and to assist in maintaining security, confidentiality, and data protection.

2.2.2 The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's 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 Any emails sent from own personal 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 may incur a penalty.

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

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

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

- use a minimum of a four-digit pin, strong pass and strong password using random words to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after six failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 2 hours
- 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 council if a device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

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

2.2.9 Personal information and sensitive data should not 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.

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

2.2.12 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.

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

2.2.14 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 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 qualified person, are offered to employees using display screen equipment. Further details are set out in the council's health and safety policy. If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Clerk or other authorised person.

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 should be generated by the IT provider.
- 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), 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

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 unauthorised passwords will be treated as a security incident.

4.1.6 Responsibility

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

The IT security provider is responsible for:

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

Monitoring

5.1.1 FPC 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 may 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 contractor if access to the data is necessary for performance of their roles. The information may also be shared with external providers 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 FPC 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) 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 unless arrangements have been made with a responsible person for them to be kept in a locked room or cabinet if they are to be left unattended at any time;
- any data should be kept safely and should only be disposed of securely;
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be

taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed;

- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft;
- Councillors, staff, and other authorised users who work away from the office with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

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

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

Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. 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 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.

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 individual.

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.

8.2 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, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the Clerk.

8.3 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. To note: 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 FPC values councillors, staff, and authorised users participating in sector discussions and improving its image through blogging and social media where relevant to their role. However, inappropriate comments or posts whether or not the council is mentioned can harm its reputation. Any remarks or photos that could be seen as linked to the council, abusive, discriminatory, harassing, or offensive will be treated seriously. Councillors, staff, and users should remember that parishioners and local groups may read personal weblogs for information about council matters, so all comments should be considerate even if the council is not named.

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

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of the council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a

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

9.1.4 The council may monitor social media posts. Employees must not misrepresent themselves or their council role online. Councillors, staff, and authorised users should discuss concerns directly with the council, not on social media.

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

Misuse

Misuse of IT systems and equipment 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 being taken.

Approved Full Council: 1st December 2025

Minute Reference: XXX

Review Date: May 2027

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. 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 is correct at time of 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.