

CRANLEIGH PARISH COUNCIL - STANDING COMMITTEES AND OBSERVERS ON OUTSIDE BODIES 2025/26				
Parish Council	Finance Committee (Max. 7)	Planning Committee (Max. 12)	Personnel Committee (Max. 5)	Property & Asset Committee (Max. 12)
Claire Bennett Rosemary Burbridge Trevor Cobby Mary Ann Johnson Dave Nicholas Hannah Nicholson Yvette Nicholson Marc Scully Brian Steel Liz Townsend Rowena Tyler Clive Walker**	Trevor Cobby Dave Nicholas** Marc Scully Rowena Tyler Liz Townsend Clive Walker*	Claire Bennett Rosemary Burbridge** Dave Nicholas Hannah Nicholson Marc Scully Brian Steel Rowena Tyler* Clive Walker	Rosemary Burbridge* Mary Ann Johnson Hannah Nicholson Marc Scully Rowena Tyler	Rosemary Burbridge Trevor Cobby** Mary Ann Johnson Dave Nicholas* Yvette Nicholson Marc Scully Brian Steel Clive Walker
Subject Access Request				
Dave Nicholas** Marc Scully Liz Townsend Rowena Tyler Clive Walker*				

* Chairman

** Vice Chairman

PARISH COUNCIL OBSERVERS		Observer	Reserve
Chamber of Commerce	BID rep	M Scully	
Climate Change Lead		M West	
Cranleigh Arts Centre		M Scully	
Cranleigh Brick and Tile Liaison Group		D Nicholas	
Cranleigh Community Fund		R Burbridge	
Cranleigh Health and Wellbeing		M Scully	
Cranleigh Heritage Trust		R Burbridge	
Cranleigh Library		R Burbridge	
Cranleigh Networking Group		E Townsend, R Tyler	
Cranleigh Vallendar Club		M Scully	
Cranleigh Neighbourhood Watch		D Nicholas	
Dementia Friendly Cranleigh		H Nicholson	
Destination Cranleigh		D Nicholas	
Dunsfold Advisory Group		Vacancy	
Gatwick - CAGNE		C Walker	
High Street SCC Working Party			Rowena Tyler
Internal Audit		D Nicholas, C Walker	Rowena Tyler
Knowle Park		R Burbridge, H Nicholson	
Leisure Centre		C Walker	
Older Persons Network		R Burbridge	
Performing Arts Group		B Steel	
Remembrance Day		T Cobby	
Rowleys		R Burbridge	
SALC		M Scully, C Walker	
Snnoxhall Pavilion Working Party		C Bennett, T Cobby, M A Johnson, D Nicholas, Y Nicholson, M Scully	
Surrey Police		Clerk	
Town and Parish Council meeting (Waverley) 1 Cllr plus Clerk to attend		R Burbridge, C Walker	
VJ Day		T Cobby, M Scully	
Waverley Cycle Forum		D Nicholas	
Wey & Arun Canal		R Burbridge	
Youth Council		B Bell, R Burbridge, H Nicholson, M Scully, E Townsend, R Tyler	
Youth Lead		B Bell	
Henry Smith Charity - 2 Councillors + 3 independent members		R Burbridge	
		Brian Cheesman	Cathy Gould
		C Walker	
		Roy Gasper	

If you cannot attend a meeting please ensure that you alert either the deputy or the office so that Parish Council Representation is ensured.



EMAIL AND INTERNET USAGE POLICY

Introduction

The Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

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.

Monitoring of IT Use

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

Scope of this Policy

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

Computer Use

1.1 Hardware

1.1.1 Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the clerk). Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

1.1.2 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 the Clerk.

1.1.9 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 Any faults or necessary repairs must be reported to the Clerk.

Equipment

2.1 Portable Equipment

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

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

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

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

2.1.5 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 insurance excess fee for the loss/damage.

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

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

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

2.2 Use of Own Devices

2.2.1 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.

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 However, the same security precautions apply to personal devices as to the council's desktop equipment. For continuity purposes, calls made to external parties (such as external stakeholders) must be made on council landlines or mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

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

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

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

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

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

2.2.12 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 IT provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.14 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, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

3.1 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 VDU safe work assessment.

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

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

4.1 Password and Authentication Policy

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

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

To further strengthen account security:

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

For more guidance, see the NCSC's advice on password security: [NCSC Password Guidance](#)

4.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the chair of council, in a sealed envelope, only to be accessed in an emergency.

4.1.3 Password Storage and Management

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

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

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

4.1.6 Responsibility

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

The IT security provider is responsible for:

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

5.1 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 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 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.

6.1 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 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 non council premises unless arrangements have been made with a responsible person at 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.

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

7.1 Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

7.1.2 On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

7.1.3 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask the IT provider, rather than assuming they know the right answer.

7.1.4 All councillors, staff, and other authorised users who need to use email as part of their role will normally be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

7.1.5 Email messages sent on the council's account are for council use only. Personal use is not permitted.

8.1 Use of the Internet

Copyright

8.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

8.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

8.1.3 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

8.1.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

8.1.5 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the clerk if unsure about anything.

9.1 Network and Internet Usage

Cranleigh Parish Council's network and internet connections should be used responsibly and efficiently for official purposes.

9.1.1 Staff members are encouraged to use the internet responsibly as part of their official and professional activities.

9.1.2 Information obtained via the internet and published in the name of the Council must be corroborated as accurate and valid according to recognised government, educational, or standards of UK Publishing regulations.

9.1.3 Information obtained via the internet and published in the name of the Council must be relevant and professional. A disclaimer must be stated where personal views are expressed.

9.1.4 The use of the internet to access and/or distribute any kind of offensive material will not be tolerated and staff may be subject to disciplinary action.

9.1.5 The equipment, services and technology used to access the internet must only be those authorised for this purpose by the council, or the property of the council. The council reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections.

Unacceptable use of the Internet

Unacceptable use of the internet by staff members includes, but is not limited to:

- sending or posting discriminatory, harassing or threatening messages or images
- using computers to perpetrate any form of fraud, and/or software, film or music piracy
- obtaining, using or disclosing another staff member's password without authorisation
- sharing confidential material or proprietary information outside of the council
- hacking into unauthorised websites
- sending or posting information that is defamatory to the council, its services, councillors and/or members of the public
- introducing malicious software onto council computers and/or jeopardising the security of the council's electronic communication systems
- sending or posting chain letters, solicitations or advertisements not related to Council business or activities
- passing off personal views as those representing the Council
- accessing inappropriate internet sites, web pages or chat rooms
- Creating accounts on Social Media or other services on behalf of the council without the authorisation of the Council or responsible officer.

If a staff member is unsure about what constitutes acceptable internet usage, then he/she should ask his/her line manager for further guidance and clarification

9.2 Trademarks, links and data protection

9.2.1 The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the clerk.

9.2.2 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 included in the Staff Handbook.

9.3 Accuracy of information

9.3.1 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.

10.1 Use of social media

10.1.1 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.

10.1.2 Personal use of social networking/media and chat sites are not permitted during working hours.

10.1.3 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.

10.1.4 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:

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of the council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council.") Writers must not claim or give the impression that they are speaking on behalf of the council.
- Any employee who is developing a site or writing a blog that will mention the council, e.g. "our current or potential plans, councillors, staff, and other authorised users, partners, must inform the clerk that they are writing this and gain agreement before going 'live'.
- The council expects councillors, staff, and other authorised users to be respectful about the council and its current or potential 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 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 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 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.

10.1.5 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.

10.1.6 It is important to note that 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 external stakeholders contact details from any personal device/equipment.

11.1 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.

12.1 Reporting and Sanctions

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

12.1.1 If a Councillor receives an email from a staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will consider use of the Council's formal disciplinary procedure, or refer the matter to the Personnel Committee depending on the severity of the event.

12.1.2 If a staff member receives an email from another staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will consider use of the Council's formal disciplinary procedure, or refer the matter to the Personnel Committee depending on the severity of the event.

12.1.3 If a staff member receives an email from a Councillor which they believe is contrary to the guidance provided in this policy, the staff member is entitled to consider use of the Council's grievance policy and/or report the issue through the procedures outlined in the Member's Code of Conduct.

13.1 Compliance and Consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

14.1 Training and Awareness

Cranleigh Parish Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

15.1 Policy Review

Updates may be made to address emerging technology trends and security measures.

16.1 Contacts

For IT-related enquiries or assistance, users can contact the Clerk in the first instance.

All staff and councillors are responsible for the safety and security of Cranleigh Parish Council's IT and email systems. By adhering to this IT and Email Policy, Cranleigh Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

December 2025

Policy Review Date: October 2026

COMMONS ACT 2006 – SECTION 38*

We are applying to the Secretary of State for Environment, Food and Rural Affairs (Defra) for consent to construct works on **Cranleigh Common** under section 38 of the Commons Act 2006. The Planning Inspectorate will determine the application on behalf of Defra.

We are required to give you notice of our proposals and are sending you a copy of the attached notice in order to comply with that requirement.

[For section 38 applications only:

Under section 38, we need Defra's consent to carry out any restricted works on **land registered as common land** under the Commons Registration Act 1965 or the Commons Act 2006 (and on certain other land specified in section 38).

Restricted works are any that prevent or impede access to or over the land. They include fencing, buildings, structures, ditches, trenches, embankments and other works, where the effect of those works is to prevent or impede access. They also include, in every case, new tarmac (or similar) surfaces, such as for a new car park or access road.]

Defra's decision will be based on the merits of the proposal, and will balance all the interests in the common, taking account of all views expressed. Regard must be given to the criteria set out in section 39 of the Commons Act 2006. These are:

- (a) the interests of persons having rights in relation to, or occupying, the land (and in particular persons exercising rights of common over it);
- (b) the interests of the neighbourhood;
- (c) the public interest, which includes the public interest in:
 - nature conservation
 - the conservation of the landscape
 - the protection of public rights of access to any area of land, and
 - the protection of archaeological remains and features of historic interest;
- (d) any other matter considered relevant.

These criteria will be viewed in the light of the overriding objective of protecting, maintaining or improving the common, and of ensuring that the overall stock of common land is not diminished. This will enable the diversity, variety, and overall extent, of common land to be safeguarded.

Any representations about the proposal should be sent to the Planning Inspectorate by the closing date specified in the notice.

Find, save and share **Public Notices** that affect you in your local area.

Stay informed...


**Public Notice
Portal**
To place a public notice, please email: publicnoticesteam@reachplc.com visit publicnoticeportal.uk

Planning

RUSHMOOR BOROUGH COUNCIL TOWN AND COUNTRY PLANNING ACT 1990 ARTICLE 15 OF THE TOWN AND COUNTRY PLANNING (DEVELOPMENT MANAGEMENT PROCEDURE) (ENGLAND) ORDER 2015 TOWN AND COUNTRY PLANNING (ENVIRONMENTAL IMPACT ASSESSMENT) REGULATIONS 2017

The Council has received the application(s) below, which require advertising under one or more of the above Acts:-

The following application is accompanied by an Environmental Statement, and does not accord with the provisions of The Development Plan in force in the area in which the land to which the application relates is situated.

25/00615/REV - Variation of Conditions 2 (aircraft movements) and 6 (aircraft weight), and replacement of Conditions 7 (1:10,000 risk contour) and 8 (1:100,000 risk contour), of planning permission 20/00871/REVPP determined on the 22/02/2022, in order to:

a) increase the number of non-weekday aircraft movements from 8,900 to 13,500 per annum, and b) amend the permitted annual flight movements weight category from 50,000-80,000 kg to 55,000-80,000 kg, retaining the overall cap of 1,500 movements (within this cap: aircraft between 50,000-55,000 kg that do not meet ICAO Chapter 14 (or equivalent) noise standards shall continue to be counted, and non-weekday movements within the revised category shall increase from 270 to 405), and to

c) replace Conditions Nos. 7 (1:10,000 risk contour) and 8 (1:100,000 risk contour) with a new condition to produce Public Safety Zone maps in accordance with the Department for Transport Requirements at Farnborough Airport Farnborough Road Farnborough

The application is available for inspection on our website www.rushmoor.gov.uk/publicaccess

You may also inspect copies of the application, the plans, the environmental statement and other documents submitted with the application at:

1. the Council's offices: Rushmoor Borough Council, Council Offices, Farnborough Road, Farnborough, GU14 7JU during opening hours between 9am and 2pm Monday to Friday;
2. Aldershot Library: 109 High Street, Aldershot, GU11 1DD during opening hours (Monday 9.30am to 1.30pm, Tuesday, Wednesday, Friday and Saturday, 9.30am to 5pm); and
3. Farnborough Library: Pinehurst, Farnborough, GU14 7JZ during opening hours (Monday, Wednesday, Thursday, Friday and Saturday, 9.30am to 5pm and Tuesday 9.30am to 1.30pm).

Any comments on the application should be made in writing and received by 30th December 2025. Comments can be submitted through a link on our website.

Timothy Mills, Executive Head of Property and Growth
28.11.2025

Town and Country Planning (Development Management Procedure) (England) Order 2015 NOTICE UNDER ARTICLE 13 OF APPLICATION FOR PLANNING PERMISSION

Proposed development at: 170 Station Road, Addlestone, Surrey, KT15 2BD
Take notice that application is being made by: Arjun Rajawat of J2AO Developments Ltd

For planning permission to: Redevelopment of rear yard area with three storey building comprising 3 x flats, communal amenity space, refuse storage and cycle storage
Local Planning Authority to whom the application is being submitted: Runnymede Borough Council, Civic Centre, Station Road, Addlestone, Surrey, KT15 2AH
Any owner of the land or tenant who wishes to make representations about this application, should write to the council within 21 days of the date of this notice.

Signatory: Arjun Rajawat

Date: 20 November 2025

Statement of owners' rights: The grant of planning permission does not affect owners' rights to retain or dispose of their property, unless there is some provision to the contrary in an agreement or lease.

Statement of agricultural tenants' rights: The grant of planning permission for non-agricultural development may affect agricultural tenants' security of tenure. This notice is for publication in a local newspaper. 'Owner' means a person having a freehold interest or a leasehold interest the unexpired term of which is not less than seven years. 'Tenant' means a tenant of an agricultural holding any part of which is comprised in the land.

Guildford Borough Council

The Local Planning Authority has received the following applications for a Major Development, a Development Affecting a Listed Building, a Building in a Conservation Area, Historic Park & Garden or a Departure. These applications may be viewed online at www.guildford.gov.uk or at Millmead House during normal office hours. Representations should be made in writing within 21 days of the publication date of this notice to Director of Planning and Regeneration, Planning Services, Guildford.

25/P/01368 Land at Hammersley Drive, Ash
Erection of a three storey building comprising a 70 bed care home (Class C2) and associated access, car and cycle parking and landscaping. **25/P/01474 Land to the east of, Eashing Lane, Godalming**
Residential development comprising of 234 dwellings, including 50% affordable dwellings, together with means of access, internal road network, parking, public open space (including play space), landscaping and associated works. (Application for Full Planning Permission). **25/P/01490 24 Sandfield Terrace, Guildford**
Enlargement of existing basement lightwell to provide a means of escape in connection with basement conversion. **25/P/01497 Brae Lea, 3 Austen Road, Guildford**
Erection of a two-storey dwelling and outbuilding together with new boundary treatment and vehicular access following the demolition of existing garage and boundary wall.

25/P/01531 47 The Street, Shalford, Guildford
Listed Building Consent for the erection of a tiled patio and timber pergola garden structure. Proposed aluminium bifold doors to replace existing side window and replacement of a number of existing windows across the front & rear elevations and removal of existing wall dividing kitchen and dining room. Proposed internal timber stud wall to divide entrance hall to dining room. **25/P/01537 10 Orchard Road, Shore, Guildford**
Erection of two storey side/rear extension with open canopy porch, and alterations to front landscaping, following demolition of existing porch, garage, car port and rear two storey studio. **25/P/01542 31 Longmead, Guildford**
Application under Section 73 of the Town and Country Planning Act 1990 to vary condition 2 (approved drawings) to create a loft room with 3 roof lights of planning permission 25/P/00275 for the 'Erection of an additional storey above the main part of the house and erection of a single storey side extension following removal of existing garage'. **25/P/01543 Holm House, The Street, West Clandon**
Erection of a car port.

CRANLEIGH COMMON

University of Surrey has applied to the Secretary of State for Environment, Food and Rural Affairs for consent under section 38 of the Commons Act 2006 to carry out restricted works on Cranleigh Common. The Planning Inspectorate will decide the application on behalf of the Secretary of State.

The proposed works are: Installation of self-standing metal pole (3 metres in height and 10 cm in diameter, securely fixed to a weighted base. A solar-powered environmental and water-quality sensor (30 x 20 x 15 cm; weight 3 kg) will be mounted on top. The total installation footprint is under 1m2.

The works will be located Cranleigh High Street (Fountain Square), Cranleigh, Surrey GU6 8AJ

A copy of the application form and accompanying documents can be inspected at Cranleigh Post Office 41 High Street, Cranleigh, GU6 8AP during normal office hours until 31 December 2025. A copy of the application form and accompanying documents may be obtained by writing to Dr. Anubhav Dwivedi Global Centre for Clean Air Research (GCARE), University of Surrey, Guildford, GU2 7XH

Email: a.dwivedi@surrey.ac.uk

Any representations should be sent in writing ON or BEFORE that date to The Planning Inspectorate, Commons Team at 3A Temple Quay House, Temple Quay, Bristol, BS1 6PN or commonlandcasework@planninginspectorate.gov.uk. If you use artificial intelligence (AI) to create or alter any part of documents, information or data submitted with a representation, you should tell The Planning Inspectorate that you have done so when you submit it. See the detailed Use of artificial intelligence in casework evidence guidance for further information.

Representations sent to The Planning Inspectorate cannot be treated as confidential. They will be copied to the applicant and possibly to other interested parties. To find out more about how the Planning Inspectorate uses and manages personal data, please go to the privacy notice.

Anubhav Dwivedi
Global Centre for Clean Air Research (GCARE)
University of Surrey
Guildford GU2 7XH
28 November 2025



The Local Planning Authority has received the following applications for a Major Development, a Development Affecting a Listed Building, a Building in a Conservation Area, Historic Park & Garden, or a Departure. Copies of Planning Applications are available for inspection on our website www.waverley.gov.uk/planning. Representations should be submitted to the Head of Planning in writing at Waverley Borough Council Offices, The Bury, Godalming, GU7 1HR within 21 days of the publication of these notices. Comments can be submitted through a link on our website.

WA/2025/02238 Application under S73 to vary condition 1 (approved plans) of WA/2022/03084 to make alterations to the design. **Furzons Cottage Rosemary Lane Alfold Cranleigh GU6 8EY.**

PIP/2025/02242 Technical Details consent pursuant to Permission in Principle PIP/2024/01818 (as amended by NMA/2025/00449) for the erection of 5 detached dwellings and associated infrastructure. **Plot Community Building Land Comprising Of 5 Fields South Of Amlets Lane Cranleigh.**

PIP/2025/02251 Technical Details consent pursuant to Permission in Principle PIP/2024/01353 for the erection of a dwelling with associated works, solar roof panels including a new vehicular access. **Land Adjacent to Burstowes Croft the Green Ewhurst Cranleigh GU6 7RT.**

WA/2025/02258 Change of use, extensions and alterations to existing single storey office building (Use Class E) to provide a two-storey building containing 4 residential units (Use Class C3) with amenity space and parking; demolition of north facing single storey projection. **Unit 1 Miltons Yard Petworth Road Godalming GU8 5LH.**

WA/2025/02266 Listed Building Consent for repointing and chimney repair works; replacement of fireplace with an inglenook fireplace. **Bildens Farm Gadbridge Lane Ewhurst Cranleigh GU6 7RW.**

WA/2025/02276 Alterations to flats 1 and 2 to provide a single dwelling together with erection of a garden shed. **Flats 1 And 2 The Tannery Station Approach Godalming GU7 1FW.**

28 November 2025



The following applications have been received for proposals which affect a Listed Building, Conservation Area or notice under Article 8 (Major Developments). Details may be inspected at the Town Planning Division, Civic Centre, High Street, Esher between 8.45am and 5.00pm Monday to Friday. Any written representations to be made to me within the 21 days of publication of this notice. Please note that in accordance with the Local Government (Access to Information) Act 1985, any representations received will be made available for public inspection. The application plans and details will be displayed on the Council's Website at www.elmbridge.gov.uk

Kim Tagliarini

Strategic Director Date of Issue: 21st November 2025

2025/2659 FUL The Old Post House 91 Heath Road Weybridge Surrey KT13 8TS

First floor rear extension of a dental practice to be used as a dental hygiene room.

2025/2660 S73 51A Palace Road East Molesey Surrey KT8 9DN

Variation of Conditions: 2 (Approved Plans) and 11 (Vehicle Parking) of planning permission 2024/1350 (Detached two-storey house with rooms in the roof space, basement, and bin and cycle stores following demolition of existing house) to revise internal layout, amend the orangery, to alter the dormer windows, rooflights, fenestration and materials and to alter the wording of Condition 11 to remove requirement of vehicles being able to turn within the site boundary so that they may enter and leave the site in forward gear.



Love being part of
something local

marketplacealive.co.uk

Runnymede Borough Council

Town and Country Planning Act 1990, The Planning (Listed Buildings and Conservation Areas) Act 1990: The following applications have been received for proposals which may affect a Listed Building and/or a Conservation Area, may be a Major Development and/or a Departure from the Development Plan, and/or affect a public right of way or an Environmental Statement has been submitted. Details may be inspected online at www.runnymede.gov.uk. Any representations must be done by going through the planning search on the Council website and pressing 'make a comment', this needs to be received within 21 days from the publication of this notice; one additional day will be given for each Bank Holiday falling within this period. Representations received are available for public inspection.

RU.25/1213 Centrum House, 36 Station Road, Egham, Surrey, TW20 9LF Removal of the existing mansard roof structure and create additional floors to accommodate 21 self-contained residential apartments.
RU.25/1618 Woburn Hill Nursery, Woburn Hill, Addlestone, Surrey, KT15 2QG Variation of Condition 2 (approved plans) of planning permission RU.22/1535 to reflect an M4(3) wheelchair compliant design for 4 no. dwellings (erection of 74 residential dwellings with associated parking, landscaping, and drainage features following the demolition of garden centre buildings)

Dated: 28th November 2025, Victoria Gibson - Development Manager on behalf of Runnymede Borough Council

SURREY HEATH BOROUGH COUNCIL

NOTICE IS HEREBY GIVEN that the following applications have been received for proposals which may affect a Listed Building and/or a Conservation Area, affect a Public Right of Way, be a Major Development, or a Departure from Development Plan. Details of these applications, can be inspected online at www.surreyheath.gov.uk (Planning and Building) or in the Contact Centre, Surrey Heath House, Knoll Road, Camberley, between 9.00am and 5.00pm Monday to Thursday and 9.00am and 4.30pm on Friday. Representation should be made in writing within 21 days of the publication date of this notice to the Head of Planning. Please note that in accordance with Local Government (Access to Information) Act 1985, any representations received will be made available for public inspection.

25/1127/FFU Windlesham Hub, Field Of Remembrance, Kennel Lane, Windlesham

Erection of a single-storey timber outbuilding for additional nursery accommodation.

25/1123/FFU 80 High Street, Chobham
Change of use of part of ground and first floor from retail storage (Class E) to residential (Class C3) to form one flat over two floors, and creation of additional flat (Class C3) at first floor along with associated internal and external alterations including creation of a roof terrace.

Keiran Bartlett,
Head of Planning

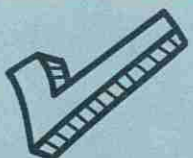
28th November 2025

BOROUGH OF SPELTHORNE TOWN PLANNING SERVICES

The following applications have been received for proposals which may affect a Listed Building and/or a Conservation Area, or which may be a 'major development'. The application is available for inspection online at the Council's website www.spelthorne.gov.uk. Any written representations to be made to me within 21 days from the publication of this notice. Please note that in accordance with the Local Government (Access to Information) Act 1985, any representations received will be made available for public inspection: Group Head of Place, Protection and Prosperity on behalf of Planning Development Manager.

Date of issue - 28.11.25

25/01267/ADV and 25/01266/FUL - Halford School, Russell Road, Shepperton, TW17 9HX - Erection of an 8 m flag pole to display a Halford School flag and an advertisement consent for a Halford School flag. These applications affect the Setting of the Grade II Listed Building and the site is located in the Lower Halford Conservation Area.



Any item any price free online

marketplacealive.co.uk

**SNN/2024/0530 - potential new road name at site of land to rear of LITTLE PARK HATCH,
BOOKHURST ROAD, CRANLEIGH**

From addressing@waverley.gov.uk <addressing@waverley.gov.uk>

Date Thu 2025-12-04 11:06

To Beverley Bell – Cranleigh <clerk@cranleigh-pc.gov.uk>

Good morning,

We hope you are well.

We have an addressing application for the 6 new dwellings at the above location.

We will create a new road name to address the new properties.

We wondered if you have any road name suggestions based on your local knowledge and the history of the site?

Please could you let us know if you have any suggestions (remembering that road names cannot be duplicated within the borough).

We have previously discussed the following road name prefixes for new roads in Cranleigh: CANDLE, FOUNTAIN, TINDERBOX, SPARKLER, LANTERN, GUNPOWDER, HOT COALS - are any of these of interest? Please let us know and we will do full checks on them.

We look forward to hearing from you with your suggestions.

Could you also let us know what you believe is happening with LITTLE PARK HATCH, BOOKHURST ROAD, CRANLEIGH - is this an empty property? We have looked but can't see any recent planning permissions for this property and wondered if you had any knowledge about the property.

Kind regards,

Elizabeth Silley

Address Development Team
01483 52 3507