HOUGHTON REGIS TOWN COUNCIL

Information Technology Policy

Date of Approval:	23rd October 2006
Reviewed:	27th February 2013; 11th June 2018; 1st March 2021; 3rd March 2025
Date of Re approval:	8th October 2018; 22nd March 2021; 16th June 2025

Contents

1 Purpose 3
2 Scope 4
3 Computer use 4
3.1 Hardware 4
3.2 Portable IT equipment 5
3.3 Phones 6
3.4 Video Conferencing 6
3.5 Use of own devices including BYOD (Bring Your Own Device) 6
4 Health and safety 8
5 Software 8
6 Virus checking 9
7 Desktop appearance and settings 9
8 User IDs and passwords 10
9 Files and data 11
10 Monitoring 11
11 Remote working 12
12 Email 13

12.1 General principles 13
12.2 Reading email 14
12.3 Sending email (including replies and forwarding) 14
12.4 Legal proceedings and libel 17
12.5 Carbon copying (CCing) 17
12.6 Attachments 17
12.7 Deleting and storing email 17
12.8 Chain mail 18
12.9 Spam/junk mail 18
12.10 Specifically prohibited activities 18
12.11 Security 18
12.12 Accessing other email accounts 19
12.13 Monitoring of emails 19
13 Use of the Internet 19
13.1 General principles 19
13.2 Copyright 20
13.3 Trademarks, links and data protection 20
13.4 Accuracy of information 21
13.5 Downloading material 21
13.6 Registering on external web sites 21
13.7 Personal use 21
13.8 Misuse of the Internet 22
13.9 Removing internet access 23
14 Houghton Regis Town Council website 23
15 Use of social media 23
16 Training 26
17 Breach of this policy 26
18 Related policies and documents 26
19 Further information 26
20 Policy owner 27

1 Purpose

1.1 IT communications are a key part of Houghton Regis Town Councils business, and so it is important that we adhere to certain standards to protect everybody. Our IT systems and services are primarily a business tool and we aim to take a fair and consistent approach to their use within our organisation. This policy sets out the rules when using our computer equipment and systems. Computer equipment includes laptops, stand-alone PCs and other portable devices. This policy also covers system security, personal use, computer viruses, monitoring, email and internet use, and what we would deem to be inappropriate use.

1.2 We also expect employees and workers to maintain a high standard of conduct whilst using the organisation's IT systems and associated facilities.

1.3 We operate a zero-tolerance policy on any form of bullying, harassment, sexual harassment or discrimination during the course of employment, including when using IT systems and associated facilities. It is expected that employees and workers and workers using our systems to treat colleagues and others with respect and to behave in a way that does not conflict with our policies, work activities, business dealings or which may adversely affect or undermine our reputation.

1.4 We encourage employees to use email at work. However, we do require them to follow the simple rules below and to note that a serious breach of these rules could lead to dismissal. Any employee or worker who is unsure about whether anything may be in breach of these rules should speak to their Line Manager in the first instance.

1.5 Misuse of the Internet or email may give rise to legal liability to third parties. It may also give rise to a claim against us. Unauthorised access or intentional modification to restricted documentation or software will be considered a disciplinary offence. By following the standards set out in this policy, we aim to ensure that the use of our IT equipment and services are legally compliant and secure and that our users can work efficiently and productively. It is therefore vital that this policy is adhered to.

1.6 It is important that all users understand their responsibilities and are aware of the implications of misuse of our systems and services. The purpose of this policy is to ensure that all users are aware of the restrictions that we place on the use of our IT systems and services, and the implications that misuse of it might have on the individual and Houghton Regis Town Council. .

1.7 If there is anything in this policy which becomes unworkable or unclear, then this must be brought to the attention of the employees Line Manager

1.8 The current laws must be obeyed at all times. We will never ask nor expect any employee to breach the law whatever the circumstances.

1.9 IT and the law relating to it changes all the time and this policy will be updated regularly. Users are responsible for ensuring they read and understand the latest version of this policy which will be emailed or printed off for employees.

1.10 This policy should be read together with our Disciplinary Policy, Grievance Policy, Equality, Diversity and Inclusion Policy, Bullying and Harassment Policy, and Social Media Policy which will be emailed or printed off for employees as well as being available on the Town Council shared drive.

1.11 This policy is not contractual but sets out our current rules and procedures for computer, email, and internet use.

2 Scope

2.1 This policy applies to:

- HRTC employees and\or Councillors
- Houghton Regis Town Council IT equipment including (but not limited to) computers, tablets, laptops, printers, mobile phones and network
- Software and IT services licensed by Houghton Regis Town Council
- Volunteers using Houghton Regis Town Council computer equipment and\or network.
- Councillors when using Houghton Regis Town Council IT equipment and\or network.
- Members using social networking media in their capacity as Councillors

2.2 New employees must be made aware of this policy upon joining Houghton Regis Town Council as part of the induction process.

2.3 Any Houghton Regis Town Council employee and\or Councillor who are requesting permission to use their own IT equipment (e.g. mobile phones, tablets) for Council business purposes.

3 Computer use

3.1 Hardware

3.1.1 Our IT equipment and services are provided for Houghton Regis Town Council business purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of a Senior Manager). Any personal use of our IT equipment and services should not interrupt our daily business in any way and users are asked to restrict any personal use to official lunch breaks or before or after working hours.

3.1.2 All IT equipment supplied should be treated with good care at all times. IT equipment is expensive, and any damage will have a financial impact on the Council.

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

3.1.4 All IT equipment will carry a number which is logged against the current user of that equipment. A database of IT equipment issued will be kept.

3.1.5 IT equipment should not be dismantled or reassembled without seeking advice.

3.1.6 Employees are not to purchase any IT equipment or software for Houghton Regis Town Council without it being authorised by a Senior Manager

3.1.7 Personal external storage devices, e.g. USB disks, CDs, DVDs, memory sticks, cannot be used on our computers without the prior approval of a Senior Manager.

3.1.8 Any IT faults or necessary repairs must be reported to a Senior Manager or to the company who provide IT support to Houghton Regis Town Council, currently Techies Ltd.

3.2 Portable IT equipment

3.2.1 Portable IT equipment includes, but not limited to, laptop computers, notebooks, tablets, mobile phones., external storage devices.

3.2.2 Data backup procedures specific to portable IT equipment should be followed at all times.

3.2.3 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 IT equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times and must not be left unattended when away from our premises. and should never be left in parked vehicles.

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

3.2.5 If an item of portable IT equipment is lost or damaged this should be reported to a Senior Manager. If the loss or damage is due to an act of negligence by the user, they may be liable to meet an agreed amount of the loss/damage.

3.2.6 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 our premises without the prior written permission of a Senior Manager. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

3.2.7 Under no circumstances must any meeting or conversation be recorded without the express permission of those present.

3.2.8 In addition, we do not permit-webcams to be used in the workplace, other than for conference calls for business purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from a Senior Manager

3.3 Phones

3.3.1 Houghton Regis Town Council use a phone system (3CX) that connects to the internet to make and receive phone calls (both internal and external). The system can be accessed either through a web browser or an application that is installed on any compatible device.

3.3.2 If the user is making a business call from a mobile phone (both Houghton Regis Town Council and personal device) then the call should be made from the 3CX system rather than the mobile number unless this is unavoidable.

3.3.3 If a 3CX phone user is not available (e.g. holiday) then the status of the users extension should be changed to show this, and an appropriate call forwarding is set.

3.3.4 Personal calls must not be made from the 3CX system as this will show Houghton Regis Town Council as the caller ID.

3.3.5 The status must be set to available during working hours except if permission has been obtained to change it by a manager.

3.3.6 Automatic call forwarding to another user must only be setup if the user the call is being forwarded to has agreed to this.

3.4 Video Conferencing

3.4.1 Video conferencing is available from many different applications (including Microsoft Teams, Zoom and 3CX).

3.5 Use of own devices including BYOD (Bring Your Own Device)

3.5.1 Some users may wish to use their own smartphones, tablets, laptops etc. to connect to the Town Councils network. and use them for business purposes. This includes, but not limited to, reading Town Council emails, accessing Town Council documents stored on our server(s) or access data in other services. Any such use of personal devices will be at the discretion of the user's manager, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices must be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

3.5.2 The same security precautions apply to personal devices as to Town Council owned IT equipment. For continuity purposes, calls made to external parties must be made on our 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 include our name, address, contact telephone number and our standard disclaimer and should not identify the employee's personal email address.

3.5.3 Users of our IT services are expected to use all IT equipment (both Town Council and personal devices including mobiles) in an ethical manner and in accordance with this policy. Accessing inappropriate websites or services on any device using the Town Councils IT services that are paid for or provided by us carries a high degree of risk, and, for employees, will result in disciplinary action, including dismissal, irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

3.5.4 In cases of legal proceedings against Houghton Regis Town Council, we may need to temporarily take possession of any employee's personal device to retrieve the relevant data.

3.5.5 Wherever possible the user should maintain a clear separation between the personal data processed on our behalf and that processed for their own personal use, for example, by using different applications (apps) for business and personal use. If the device supports both work and personal profiles, the work profile must always be employed for work-related purposes.

3.5.6 Users who intend to use their own devices via any Town Council IT service must ensure that they:

- use a 4 digit pin, strong password (i.e. one which contains lower and upper case letters and numbers or fingerprint (preferably the latter) to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after 3 failed login attempts.
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 2 minutes duration
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email)
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the employee's personal data. Employees are advised therefore to keep personal data separate from business data where possible.
- ensure that they use secure WiFi networks
- be cautious if family or friends use the device, ensuring that work-related data cannot be accessed
- inform us if their device(s) is/are lost, stolen or inappropriately accessed where there is risk of access to our 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.

3.5.7 Any Town Council work done on a user's own equipment must be stored securely and password protected and must always be backed up in accordance with our standard backup procedures.

3.5.8 If transferring data, either by email or by other electronic 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.

3.5.9 Prior to the disposal of any device that has Town Council data stored on it, and in the event of a user leaving our employment, users are required to allow the Town Clerk access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

3.5.10 Users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing our 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. We will use reasonable endeavours to assist, but users are personally liable for their own device(s) and for any costs incurred as a result of the above.

3.5.11 By connecting a personal device to any Town Council network or service the user is allowing Houghton Regis Town Council to implement policy(s) on the device that will enable Houghton Regis Town Council to erase any or all of the data on the device to ensure confidentiality.

4 Health and safety

4.1 Users who work in our offices will be provided with an ergonomically designed workstation.

4.2 We have 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 our Eyecare Policy.

4.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to their Line Manager.

4.4 If any hazards are detected at a workstation, including ‘noises’ from the IT equipment, this should be reported immediately to a Senior Manager.

5 Software

5.1 Equipment allocated to individuals will be supplied with the appropriate software and configuration. Users are not permitted to load screensavers/software from any source without the prior permission of a Senior Manager.

5.2 Any software that is additional to that supplied must be discussed with the user’s manager and authorised prior to purchase to ensure that the necessary licences are also purchased.

5.3 Non-approved software or data, such as games, screen savers, video clips, non-worked related programmes, must not be installed on our computers under any circumstances, unless prior approval has been given by the Line Manager.

5.4 Copies of any software must not be made unless prior approval has been given by the Line Manager. We do not allow the use of pirated or copied computer software. All software must be licensed.

5.5 The licence agreement that accompanies software packages should be strictly adhered to. Unauthorised copies of software must not be made for use within the office or outside.

6 Virus checking

6.1 Virus protection and awareness of the importance of this is vital to our day-to-day ability to operate effectively. A catastrophic failure of the IT structure will potentially render us inoperable. Any activity by an individual that contributes to such a potential situation may result in disciplinary action, including dismissal. Users should note that the intentional introduction of viruses is a criminal offence under the Computer Misuse Act 1990.

6.2 Anti-virus software is installed on all computers and should be left running automatically and updated when prompted. Full system auto scans are set to run and must be left in place until a time when an alternative might be considered appropriate. We use virus detection software to scan all email and attachments received from any external source.

6.3 There is a risk of importing computer viruses if programmes or executable files are downloaded from the Internet, or if email attachments containing viruses are opened. All incoming email documents are scanned for viruses, and documents containing known viruses are intercepted. However, users who believe an attachment is suspicious should contact their Line Manager or the IT Support company before opening this.

6.4 All incoming material should be checked for viruses, whether loaded manually (e.g. from CDs or memory sticks) or downloaded from an external source such as the Internet before being saved or copied onto our computers.

6.5 Users must not change or install any software on their computer that includes the transference of data/software from their work or home computer without the express permission of the Town Clerk.

6.6 If a virus is detected a Senior Manager or the IT Support company must be notified immediately.

6.7 Nothing should be attached to an email which may contain a virus. We could be liable to the recipient for any loss suffered. We have virus-checking in place, but a check should be made with a manager if in doubt.

6.8 Care should be taken when forwarding attachments from third parties, particularly unidentified third parties. These may carry viruses, and they may also not have been cleared for copyright issues. Sending them on to someone else may be a breach of copyright and result in damages for breach of copyright.

7 Desktop appearance and settings

7.1 The programme and desktop icons should not be changed from the standard icons.

7.2 Our IT systems may not be used to acquire, display or distribute any content that may be considered offensive to others, including content of a sexual nature. This includes, but not limited to, any programme, image, document, sound or video clip that can be displayed or heard on any IT equipment.

7.3 Sound systems on computers must be switched off in consideration of people working near to you.

8 User IDs and passwords

8.1 Users are authorised only to use the IT services made available to them when logging onto the IT equipment under their allocated username.

8.2 Individual users are responsible for the security of their IT equipment and must not allow this to be used by an unauthorised person. Personal password(s) should be kept confidential and all reasonable precautions taken to prevent unauthorised access to the data stored on any Town Council IT equipment.

8.3 Users are not permitted to use, change or divulge to any other party, their or any other person's password or own Council system password without the express permission of a Senior Manager.

8.4 Passwords should not be written down anywhere where they could be easily retrieved by someone else.

8.5 Users should never use another person's username, email address or password (unless specifically authorised to do so), nor should they permit any other person to transmit, download, copy, forward or store material using their username, email address or password.

8.6 A user who changes their name through marriage, divorce, deed poll or any other method, should inform their Line Manager immediately so that all user IDs, passwords and email addresses can be amended accordingly.

8.7 When logged onto our IT system, and leaving any IT equipment unattended, or on leaving our workplace, users should ensure they log off the system to prevent unauthorised access. Any printed material should also be collected and stored confidentially.

8.8 Passwords may be changed from time to time, especially when someone leaves our employment.

8.9 On leaving our employment, access to our systems will be immediately withdrawn. Incoming emails will be diverted to the leaver's manager and an automatic response will be set up informing the sender that the address is no longer to be used to contact the leaver. Any passwords giving remote access to our systems will be changed, thus preventing unauthorised access. We will also notify any suppliers or contractors of any leavers who should be removed from their list of those who are authorised by us to use their services. Note that in order to protect our business interests, the above may also apply during any period of "garden leave".

9 Files and data

9.1 All files should be stored on the Town Councils file servers. Permission must be obtained from the Town Clerk before any data is removed or duplicated to any other IT equipment.

9.2 Any Town Council sensitive or personal data stored on our IT equipment must be kept in the strictest of confidence and no copies must be taken other than for back-up purposes without the permission of the Town Clerk.

9.3 All reasonable precautions should be taken to ensure that any data storage devices containing Town Council files, or printouts of data are secure from theft or copying.

9.4 Any data stored on our IT equipment or systems must only contain information relating to our business. No personal data must be stored on our IT equipment and systems.

9.5 No data of any other description should be present on our computer systems with specific regard to pornographic or obscene material, whether pictorial or descriptive.

9.6 All users must be aware that storing any Town Council personal data on a computer is subject to data protection legislation.

9.7 Houghton Regis Town Council IT equipment and systems must be used responsibly and in a way that does not interfere with, disrupt or prevent anyone else legitimately using these resources. Users should ensure they are aware to which drives they have access/modification rights and remember this when saving confidential data. This is to make certain that the right people can view and edit the files saved to the system.

9.8 Unauthorised access, attempts to access, modify, delete or use data belonging to the Town Council will be considered a disciplinary matter and potentially a criminal offence under the Computer Misuse Act 1990.

9.9 Users will be notified of any data backup procedures in place that affect them: these must be followed at all times.

9.10 Hard copies should be kept of information regarded as legal messages, relating to such matters as occupancy, staff or business transactions. Financial information, including VAT records (which should be stored for 6 years), must be stored on physical files.

10 Monitoring

10.1 Houghton Regis Town Council reserves the right to monitor, inspect and maintain logs of the usage of any Town Council IT equipment or personal devices that use the Town Councils network or services to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of our protection against computer viruses, our ongoing maintenance of the system, and when investigating faults.

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

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

10.4 The information obtained through monitoring may be shared internally, including with relevant managers 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.

10.5 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.

10.6 Employees and workers 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 our Data Protection Policy.

10.7 Monitoring and the inspection of the content of any files or messages (including emails) 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.

10.8 Houghton Regis Town Council also reserve the right to monitor the internet usage, including the websites 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 us from potential damage or disrepute.

10.9 Any use that the Town Council considers to be ‘improper’, either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

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

11 Remote working

11.1 Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home or any other different venue), as follows:

- if accessing the Town Councils systems or services remotely, using IT equipment that either does not belong to the Town Council or is not owned by the user then any passwords must not be saved (cached), and the user must log out or disconnect at the end of the

session deleting all logs and history records. If this is not possible for the IT equipment being used (e.g. at an internet café), our services must not be accessed from that device.

- the location and direction of the screen must be checked to ensure the contents cannot be viewed by other people. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc.
- any data printed must be collected and stored securely
- all electronic files should be password protected, and the data saved to the Town Councils system/services when accessible
- papers, files or IT equipment must not be left unattended at a third parties premises. If this is not possible for any period, then arrangements must be made with a responsible person at the third parties premises for them to be kept in a locked room or cabinet
- any data should be kept safely and should only be disposed of securely
- papers, files, memory sticks, flash drives 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, company data should be taken into the employee's 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
- employees and workers 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.

11.2 Those issued with a mobile phone that allows WiFi access using hotspot should take note of the monthly data limit for the phone and the additional cost if it is exceeded, especially if used abroad.

11.3 The use of paid for WiFi access, for example at hotels and airports should be carefully monitored and restricted to essential business use.

12 Email

12.1 General principles

12.1.1 Our 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. Users need to be careful not to introduce viruses onto our system and should take proper account of the security advice below.

12.1.2 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. Employees are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

12.1.3 These rules are designed to minimise the legal risks we run when using email at work and to guide users as to what may and may not be done. If there is something which is not covered in the policy, users should ask their manager, rather than assuming they know the right answer.

12.1.4 All employees who need to use email as part of their role will normally be given their own Town Council email address and account. We may, at any time, withdraw email access from any employee, should we feel that this is no longer necessary for the role or that the system is being abused.

12.1.5 Email messages sent from a Houghton Regis Town Council account must be for Town Council business use only. Users are asked to restrict their personal use of emails to their personal email account(s) during official lunch breaks or before or after working hours.

12.1.6 Misuse of our email address may give rise to legal liability on the user's behalf to third parties. It may also give rise to a claim being made against the Town Council. It is therefore vital that the following policy is adhered to when using email.

12.2 Reading email

12.2.1 Email messages should be read regularly. Employees who are away from their place of work for more than a day should ensure that an appropriate message is sent automatically to senders and/or that temporary access is granted to another colleague and that emails are dealt with in their absence as appropriate. With the exception of senior managers, unless specifically requested to do so, employees are not expected to read or action their emails when on any form of leave.

12.2.2 During unplanned leave or prolonged absence, and solely where necessary, we may access and/or divert email accounts to continue the smooth operation of our business.

12.2.3 Take care before opening emails from unknown sources - this is how most viruses are introduced, and they could easily spread throughout our systems.

12.2.4 When an email is received from a sender outside the Town Councils email domain (@houghtonregis-tc.gov.uk) a banner is inserted in the email to notify the recipient that it is from an external source and that any attachments or links must be checked before opening.

12.3 Sending email (including replies and forwarding)

12.3.1 Email sent from an individual's mailbox is effectively signed by an individual.

12.3.2 Emails are merely another form of communication: in some instances, they may be the only contact that a recipient has with the Town Council and the style, appearance and content of the email will therefore influence the image that is portrayed of our organisation. Emails can appear to be a more informal type of communication, but our normal standards of presentation and content apply equally to them and the language used in the message must be courteous and professional. This includes spelling, punctuation and correctly heading each email as appropriate. All emails should therefore be checked before they are sent to ensure they don't contain typing, grammatical or spelling mistakes and to ensure the content is professional and accurate. In many cases for longer emails, it may be better to prepare the message as a draft and check it carefully before sending.

12.3.3 Messages should be concise and directed only to those on a 'need to know' basis. General messages to a wide group should only be used where necessary and the "reply all" facility should not be overused.

12.3.4 Long email trails should not be sent unless absolutely necessary and messages should only be marked as 'urgent' if they warrant immediate action. "Read receipts" and requests to acknowledge acceptance of an email further add to email traffic, so should be used sparingly. Please be mindful of the size of attachments within emails. Very large attachments can have an impact on speed and performance of the email systems and internet connections and may be rejected by one or more of the recipients. Where possible, the size of pictures should be reduced and very large files compressed into smaller files by zipping them.

12.3.5 Houghton Regis Town Council users must not solicit, send or willingly receive emails of an obscene nature, or which are intended to annoy, harass, intimidate or cause offence to colleagues or members of the public.

12.3.6 Personal or sensitive data must not be sent using email unless agreement has been received from the individual concerned or this processing is necessary to carry out public functions.

12.3.7 Houghton Regis Town Council users should regularly delete or archive emails when they are no longer current or required in order to restrict the size of their mailboxes and reduce the risk of incoming emails being rejected.

12.3.8 Houghton Regis Town Council users should be aware of the characteristics of spam and phishing emails and should not reply to or forward these emails but add the sender to their email system's Blocked Senders List.

12.3.9 Emails should contain the sender's full name and job title. All emails sent by employees must have one of the following disclaimers (as appropriate):

Please consider the environment and don't print this e-mail unless you really need to.

- **** Any opinions expressed in this email are those of the individual and are not necessarily those of Houghton Regis Town Council.

- This e-mail and any attachments hereto are strictly confidential and intended solely for the addressee. It may contain information which is privileged. If you are not the intended addressee, you must not disclose, forward, copy or take any action in reliance of this e-mail or attachments. If you have received this e-mail in error, please delete and notify the sender immediately.
- The anti-virus software used by Houghton Regis Town Council is updated regularly in an effort to minimise the possibility of viruses infecting our systems. However, you should be aware that there is no absolute guarantee that any files attached to this e-mail are virus free.***

12.3.10 Email correspondence with a third party can create a binding contract or otherwise be disclosed in legal proceedings. Where appropriate, the use of clear labelling to prevent either of these circumstances arising (e.g. the words 'subject to contract' and 'without prejudice' must be used). Statements should not be made in an email which could, intentionally or otherwise, create a binding contract or make a negligent statement.

12.3.11 Emails containing confidential information, client/customer information or any personal data should only be transmitted, copied or forwarded to authorised third parties.

12.3.12 Confidential information should not be sent externally by email. Such messages should be fully encrypted (or any attachments containing confidential information password protected and the password sent separately).

12.3.13 Delivery of email, like land mail, is not guaranteed and, if used for business-critical messages, confirmation of receipt should be requested from the recipient. Note: email 'read receipts' only confirm that the email has been flagged as read, it does not confirm the contents have been read nor does it confirm who has read it (the email could be opened by somebody else with permissions on the recipients mailbox).

12.3.14 Houghton Regis Town Council emails must not be used for spreading gossip or nuisance mail, for personal gain or in breach of any of our employment policies, such as equal opportunity, bullying, harassment or sexual harassment. Sending unwanted, abusive, discriminatory or defamatory emails can constitute bullying or harassment and will be treated as a serious disciplinary issue. This also applies to any emails sent from personal IT equipment to work colleagues or other Houghton Regis Town Council contacts.

12.3.15 Take care before sending or viewing material which may be of a hurtful, suggestive or harassing nature: it is the view of the recipient that determines whether it is inappropriate, even if the recipient was not the original addressee. When preparing an email, if the overall feeling is that you are glad you have 'got it off your chest', this is probably a signal it should not be sent. Drafts should be revisited prior to sending.

12.3.16 Anyone who receives an email message that has been wrongly delivered to his/her email address should notify the sender by returning the message to that person. If the message contains confidential information, this must not be disclosed or used.

12.3.17 Any emails that contravene this policy must be brought to the attention of the Town Clerk.

12.4 Legal proceedings and libel

12.4.1 All email messages are the property of the Houghton Regis Town Council and are treated as records of the business.

12.4.2 An email message (however confidential or damaging) may be subject to disclosure in legal proceedings or to relevant competition authorities and regulatory bodies. Claims of defamation, breach of confidentiality or contract could arise from a misuse of the system. Emails must therefore be treated like any other form of correspondence and, where necessary, hard copies retained. Even deleted emails may still be recoverable and are regarded as legitimate forms of evidence in court.

12.4.3 We can be sued for libel if inaccurate statements are made in emails which disparage other people or companies. This could lead to us having to pay damages. Therefore, all messages should be read carefully before sending and if in any doubt about what is written, the content should be checked with a manager first.

12.4.4 Users should avoid making statements which criticise our competitors or their staff, state there are quality problems with goods or services of suppliers or that state (or imply) that anyone is incompetent.

12.4.5 Neither should opinions or views be expressed that could be interpreted as misrepresenting our services or those of any other organisation with whom we deal.

12.5 Carbon copying (CCing)

12.5.1 Users should take care not to copy emails automatically to all those copied in with the original message to which they are responding. It is easy to do this but may result in a message being seen by someone that should not see this or may result in the disclosure of confidential information to the wrong person. Therefore, the automatic ‘cc-ing back’ function on the email should be disabled, and each email considered before copying people in. The use of the 'Reply' rather than 'Reply All' should be adopted.

12.6 Attachments

12.6.1 Care should be taken when opening attachments, and should any attachment produce strange or unexpected results, a Senior Manager should be notified immediately.

12.6.2 Certain types of attachments will not be allowed through our gateway.

12.7 Deleting and storing email

12.7.1 Good file management should be practiced by frequently checking the content and volume of email folders. As a guide, inboxes should only contain matters awaiting action; other items should be deleted, archived or filed.

12.7.2 Deleted email is stored temporarily in the 'Deleted Items' folder and should be emptied on a regular basis.

12.7.3 For record-keeping purposes, copies of important email (both sent and received) should be stored in an appropriate location on the shared drive.

12.8 Chain mail

12.8.1 It is prohibited to originate or distribute chain letters by email, either internally or externally.

12.9 Spam/junk mail

12.9.1 Any email message identified as spam or junk mail will be forwarded but marked that it is thought to be spam. Users can either deal with this manually or set up automatic rules.

12.10 Specifically prohibited activities

12.10.1 Houghton Regis Town Council users who are authorised to access external services and systems using Town Council IT equipment or their personal devices may not send or permit to be sent on behalf of Houghton Regis Town Council any email, attachment or posting which:

- is unlicensed software or other material that infringes the intellectual property rights of a third party
- contains information that is commercially sensitive or may have legal implications for us
- contains confidential information
- may damage our reputation or our relationships with any third party
- is defamatory about our business or any third party
- is illegal, of a sexual nature, obscene, pornographic, offensive, or is discriminatory or constitutes harassment (on any grounds of discrimination or any other unacceptable grounds), or damaging, or which may be considered by others to cause distress or is otherwise abusive or threatening
- may infringe copyright of someone else's work by copying files or data onto the Councils IT equipment or by copying to a third party
- may introduce viruses into our system
- constitutes 'junk' email or is posted to multiple groups
- invites automatic email back to us.

12.10.2 In addition, Houghton Regis Town Council IT services must not be used to search for, obtain or store information from any external network, which falls into the categories listed in 12.10.1 above.

12.11 Security

12.11.1 Users should be aware that emails are potentially insecure and others who are not the intended recipient might read messages, e.g. the recipient may forward the email on to other people.

12.11.2 Both sender and recipient should understand the risks of using email as a communication channel and agree what will and will not be sent.

12.12 Accessing other email accounts

12.12.1 Users must never access another person's email account. The only exception is where the person concerned has been authorised to access these during a prolonged absence due to holiday, ill health or some other valid reason.

12.12.2 Where such access is authorised, emails must not be sent from that person's account using the original account holder's name. If a response is required, this should be sent from the sender's own account, headed "sent on behalf of (colleague's name)".

12.13 Monitoring of emails

12.13.1 We reserve the right to monitor, at any time, all emails, including deleted emails, and the IT equipment (both Houghton Regis Town Council and personal) upon which such emails are stored and circulated. This right is reserved solely for the purposes of monitoring communications relevant to our business.

12.13.2 We will not routinely monitor emails. However, email folders will be checked when users are absent from work to ensure the continuation of service.

12.13.3 While an email that is clearly private does not fall within the definition of a communication that is relevant to our business, we maintain a right to monitor and examine such a communication where there is a reasonable suspicion that the content breaches this policy or where there are grounds for suspecting criminal activity or equivalent malpractice. When monitoring personal emails, we will, in most cases, restrict this to the address and heading of the emails. Personal emails should be clearly marked as such, and where possible we will avoid opening these unless there is a suspicion of improper use, and they form a relevant part of a disciplinary investigation.

12.13.4 We exercise this right under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following reasons: to check that this policy is being observed; that no discriminatory or offensive content appears in emails, etc; to maintain an adequate level of security for our computer systems; to detect computer viruses; and to check mailboxes of absent employees.

12.13.5 Therefore, electronic communications, storage or access should not be considered private if it is created or stored on our systems.

13 Use of the Internet

13.1 General principles

13.1.1 Utilising the vast amount of data that can be found on the Internet can be a useful resource and may be integral to some roles within our business.

13.1.2 All employees who need to use the Internet as part of their role will normally be permitted access. We may, at any time, withdraw internet access from any employee, should we feel that this is no longer necessary for the role or that the system is being abused.

13.1.3 Having access to the Internet demands a level of trust and responsibility, as websites visited can record the computer system's IP address. Users should restrict their access to websites necessary to complete their daily tasks and to consider the security implications before accessing any other sites for personal use.

13.2 Copyright

13.2.1 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 sets 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 our business and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

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

13.2.3 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).

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

13.2.5 Copyright and database right law can be complicated. Users should check with their manager if unsure about anything.

13.3 Trademarks, links and data protection

13.3.1 Our name is a registered trademark. Any employee or worker who notices anyone using the same or a similar name should let their manager know, so that we may instruct our solicitors to take appropriate action.

13.3.2 Users should not register any new domain names or trademarks relating to our names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of our web pages to any other external sites without checking first with their manager.

13.3.3 Special rules apply to the processing of personal and sensitive personal data.

13.4 Accuracy of information

13.4.1 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.

13.5 Downloading material

13.5.1 Downloading large volumes of material from the Internet onto our network can place excessive demand on computing resources. This can result in poor network performance or the temporary loss of access to IT services on the network. Such material should not be downloaded unless necessary and preferably during a period when there is little other activity.

13.5.2 Files should not be downloaded on to PCs without using virus-checking software.

13.6 Registering on external web sites

13.6.1 Many websites require registration. Employees who wish to register as a user of a website for work purposes are encouraged to do so. If there is any doubt as to whether it is appropriate to register as a user of a website for work purposes, users should check with their Line Manager. Employees must ask their manager in advance so that we are aware of what they are committing us to and to ensure the registration will not result in us being inundated with junk mail. Any boxes should be ticked to show we do not want our data used for other marketing purposes.

13.6.2 Our business email addresses should only be supplied for access to sites needed exclusively for work purposes. For any such sites, the password should be registered with the Town Clerk, who must also be notified of any change to the password.

13.7 Personal use

13.7.1 We trust users to limit their browsing of the Internet for non-business purposes. When surfing the web for personal purposes, this must only be at times that do not interfere with the performance of their role or our daily business, i.e. during breaks or after hours with permission. It must also not include visiting websites that are of a sexual nature, include sexual, obscene, pornographic, offensive content, or which may be considered by others to cause distress is prohibited. Accessing websites for these purposes may lead to disciplinary action, including summary dismissal (without notice). In the case of an agency worker, the termination of their engagement with us.

13.7.2 Personal use of the Internet for conducting financial transactions, e.g. on-line banking or for the purchasing of goods, must be restricted to out of working hours.

13.7.3 Users should not have any expectation of privacy as to their internet usage. All use can be monitored and excessive use that results in wasting our time in this way may result in the facility being withdrawn and/or dealt with in line with our disciplinary procedure.

13.7.4 All users who are allowed access to the Internet must ensure that:

- they do not access any site which will result in charges being levied to Houghton Regis Town Council for such access
- they do not use the Internet to access unlawful or inappropriate material – if unlawful or inappropriate material is accidentally accessed, the user should send an email to their manager so we know the circumstances (the access may be picked up by any monitoring system). For these purposes, unlawful material is that which breaks the law such as child pornography or harassment; inappropriate material includes searches that may not be unlawful, but which may expose us to liability for harassment, sexual harassment and discrimination by colleagues who may see the search material, such as soft pornography.
- they do not enter into any contracts or commitments in our name or on our behalf
- they do not order any goods for personal use in our name.

13.8 Misuse of the Internet

13.8.1 Those who are allowed access to the Internet at work for work purposes are expected to use it sensibly and not so that it interferes with efficient working. They may be called upon to justify the amount of time spent on the internet or the sites visited, so this should be borne in mind when browsing the internet.

13.8.2 We trust employees not to abuse the latitude we give them, but if this trust is abused, then we reserve the right to alter our policy in this respect.

13.8.3 Creating, accessing, sending, downloading or the display of inappropriate, illegal, offensive, sexual, obscene or indecent material is strictly forbidden and may lead to disciplinary action, including dismissal as a possible outcome. The accessing of and downloading of some material, for example, sexually explicit material and pornography of children is a criminal offence.

13.8.4 The creation or transmission of such material, or material which is designed or likely to cause annoyance, inconvenience or needless anxiety, is strictly forbidden.

13.8.5 Furthermore, our systems may not be used for any of the following (this list is not exhaustive but indicates the sort of usage we would consider to be unacceptable, and which may lead to disciplinary action, including dismissal as a possible outcome):

- gambling
- downloading, accessing or storing large personal files which interfere with the running of the organisation, such as photographs, videos and music
- games of any kind
- copying software for personal use or using our software (including accounting programmes and/or design programmes) for personal use
- promoting non-business related religious, charitable or political material unless authorised to do so by the Town Clerk

- sending or participating in junk mail, spam mail or chain letters (this includes forwarding jokes, cartoons and video clips to groups of people and also transmitting unsolicited commercial or advertising material that is not work-related)
- bringing our name into disrepute via social networking websites
- undertaking deliberate activities that waste staff time or networked resources
- using our business email address and misrepresenting our business
- using our name, business contacts, clients or customers for personal benefit or the benefit of any other firm, company or organisation

13.8.6 IT equipment is provided as a business tool to enable users to perform their roles effectively. We expect users to have an individual and collective responsibility not to abuse any of our IT equipment or services. Damage or serious unauthorised use of or tampering with our equipment is strictly forbidden.

13.8.7 Anyone who discovers a work colleague is abusing our internet facility should inform the Town Clerk. An employee who is found to be concealing the activities of a work colleague who is abusing our internet facilities may face disciplinary action.

13.9 Removing internet access

13.9.1 We may at any time deny internet access to any employee without giving any reason, although normally we would provide reasons.

14 Houghton Regis Town Council website

14.1 Houghton Regis Town Council website is created and amended as part of defined development projects and unauthorised amendment of information on this site is prohibited.

14.2 Anyone who sees anything on our website which is not up to date should let their manager know as, for legal and public relations reasons, we need to keep it accurate and current.

15 Use of social media

15.1 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 our systems or at home.

15.2 Personal use of social networking/media and chat sites are not permitted during working hours and should be restricted to breaks during working hours, or after hours

15.3 We recognise the importance of employees joining in and helping to shape sector conversation and enhancing our image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the employee's position, this is acceptable.

15.4 Inappropriate comments and postings can adversely affect the reputation of our organisation, even if it is not directly referenced. It should be noted that if comments/photographs are likely to be construed as linked to us or, in more direct cases, if comments about colleagues, members of the public or our business could be regarded as abusive, humiliating, sexually harassment, discriminatory or derogatory, or could constitute bullying or harassment, we will treat this as a serious disciplinary offence. Employees should be aware that other organisations may read employees' personal weblogs, to acquire information on, for example, their work, products, technical developments and employee morale. Therefore, even if the Council is not named, care should be taken with any views expressed.

15.5 Social networking media may be used by the Town Council as part of its means of communication with residents and service users. Such media will be used to represent the Council as a corporate body. Where members of the public are able to post to a social media page representing the Town Council, the pages will be monitored by Town Council officers to ensure that any offensive, inappropriate or discriminatory messages will be deleted.

15.6 Members who use social networking sites in their capacity as councillors must make it clear that they are speaking in a personal capacity and not representing the view of the Council. It is the responsibility of Members to ensure that they are adhering to the Town Council's Code of Conduct when using social networking sites.

15.7 To protect both the Council and the Councils interests, we ask that everyone complies with the following rules about social media, whether in relation to our employment or personal social networking sites, and irrespective of whether this is during or after working hours:

- Contacts from any of our databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities.
- Any blog that mentions the Council, our current or potential services, employees, partners and suppliers, should identify the author as one of our 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 our organisation 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.". 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 Houghton Regis Town Council, our current or potential, employees, members, councillors, volunteers, partners, visitors and suppliers, must inform the Town Clerk that they are writing this and gain agreement before going 'live'.
- We expect our employees to be respectful about our business and our current or potential services, employees, partners, members, councillors, volunteers, visitors and suppliers

and not to engage in any name calling or any behaviour that will reflect negatively on our 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 showing any employee or worker in uniform or other clothing that includes our name or logo and that could reflect negatively on the employee, his/her job, his/her colleagues or our business should not be posted on social media; neither should photos, videos or sound recordings taken on our property without explicit permission.
- Comments posted by our employees on any sites should be knowledgeable, accurate and professional and should not compromise us in any way.
- Inappropriate conversations with residents or third parties 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 employees, 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 business of the Council should not be posted. This includes manuals; procedures; training documents; databases; non-public financial or operational information; personal information regarding other employees or suppliers; 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.
- All employees must be aware that they are personally liable for anything that they write or present online (including on a competitor's blog, post, feed or website). They 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 any individual or company that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other employees 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, must not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the business of the Council or its employees, members, councillors, volunteers, partners, visitors and suppliers, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to our business, our current and potential products, employees, partners, customers, suppliers and competitors should be referred to the Town Clerk.
- Employees 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 our employment to show that they are no longer employed by us.

- Employees who use X.com, LinkedIn, or other social media/networking sites for business development purposes must ensure that they inform us of their password(s) so that these sites can be accessed and updated in their absence.
- Employees who have left our employment must not post any inappropriate comments about the business of the Council or our employees on LinkedIn, Facebook, X.com or any other social media/networking sites.
- Any contacts made on such sites during the course of employment will be classed as business information and thus belong to the Council. Employees will be asked to disclose contacts on LinkedIn, or any other sites, that they have made in their capacity as an employee.

15.7.1 Note that we 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 us. Employees are also advised that social media sites are not an appropriate place to air business concerns or complaints: these should be raised with a manager or formally through our grievance procedure.

15.7.2 It is important to note that any contact details and information remain the property of the Council. In addition, employees leaving our employment will be required to delete all work-related data from any personal device/equipment.

16 Training

16.1 Any employee who feels they require training to increase their understanding of the real benefits the Internet can bring to their position, or to improve their ability to use our IT equipment and services, should contact their Line Manager.

17 Breach of this policy

17.1 Failure to adhere to this policy may be a gross misconduct offence and may result in action being taken under our disciplinary policy, which could lead to dismissal. Depending on the nature of the offence it may also be necessary to notify the police.

17.2 Anyone who discovers a user abusing our IT equipment or services must inform the Town Clerk An employee who is found to be concealing the activities of a work colleague who is abusing our IT equipment or services may face disciplinary action themselves.

18 Related policies and documents

- Bullying and Harassment Policy
- Data Protection Policy
- Disciplinary Policy
- Health and Safety policy

The above list is not exhaustive.

19 Further information

19.1 Any queries or comments about this policy should be addressed to the Head of Corporate Services in the first instance.

20 Policy owner

20.1 This policy is owned and maintained by Corporate Services Committee.