



## **FLITWICK TOWN COUNCIL**

### **DIGITAL & ICT POLICY**

#### **Contents**

1. Introduction
2. General Operation
3. Compliance with Legislation
4. Security
5. Virus Controls
6. Use of Computer Equipment
7. Misuse
8. Internet
9. Use of Email
10. Social Media
11. Health and Safety
12. Protocol for the use of Flitwick Town Councils Website
13. Web Links Policy
14. Sharing Technology

Appendix 1: Digital and Social Media Policy

## **1. Introduction**

This document defines the Council's Information and Communications Technology (ICT) Policy. Digital and ICT is a key enabler for the Council, both in its ongoing day to day business processes and in supporting strategic change, particularly in the drive to 'digitise' services.

The Policy is intended to support and enable the Council's Corporate Strategy. It has 3 broad aims:

1. Customer agenda - To enable customers to access the Council's services on-line, and have their requirements fulfilled, where practical, through digital solutions.
2. Business agenda - To enable the Council to make effective use and obtain the maximum benefit from the use of ICT.
3. Technical agenda - To provide a robust, reliable, effective and resilient infrastructure for the efficient delivery of ICT; this has to be allied with new business processes designed from a digital mind-set, and with the customer in mind.

Flitwick Town Council will then, make the most of technology to ensure its services are as efficient, economic and accessible as possible, particularly where the cost of change is outweighed by the benefits. This policy compliments our Information and Data Protection Policy and Social Media Policy which can also be found in our Constitution.

This Policy is directly supplemented by four appendices which give more detail in related areas:

- Appendix 1: Removeable Media Policy.
- Appendix 2: Internet Acceptable Usage Policy.
- Appendix 3: IT Access Policy.
- Appendix 4: Social Media Policy.

The Council uses its computer, software packages and the internet (including emails and social media), to further the efficiency of its business and to provide the best service possible to its customers, partners and the public. Any disruption to the use of these facilities will be detrimental to the Authority and may result in actual financial loss. This Policy sets out how the Council intends to regulate the use of these facilities.

The Council has a duty laid down in the Data Protection Act 2018 and the General Data Protection Regulations, to ensure the proper security and privacy of its computer systems and data. All users have, to varying degrees, some responsibility for protecting these assets and complying with this policy (See also the Council's Information and Data Protection Policy).

For the purposes of this document the following definitions apply:

"Computer" (or "computer system") means any device for automatic storing and processing of data and includes mainframe computer, minicomputer, microcomputer, personal computer(whether hand-held laptop, portable, tablet, standalone, network or attached to a mainframe computer), workstation, word processing system, desk top publishing system, office automation system, messaging system or any other similar device;

"Computer data" means any information stored and processed by computer and includes programs, text, geographic, pictures, video and sound.

## **2. General Operation**

- All hardware, software, data and associated documentation produced in connection with the work of the Council, are the legal property of the Council.
- The Council will maintain external support contracts for the hardware, major items of software and provision of internet facilities as necessary.
- The Council will not knowingly breach copyright of another person.
- The Council will include an assessment of risks from its use of IT in its Business Risk Assessment.

- The Council will routinely back up its essential data off site.
- The Council will make a detailed inventory of its ICT equipment on its Asset Register and also maintain a section on digital assets.
- The Council will consider the location of equipment and provide documentation to ensure optimum physical security.
- The Council will maintain a record of relevant training for each individual user.
- The disposal of any ICT equipment, software, waste or data must be authorised, undertaken safely and securely and be properly documented.
- The Council will standardise where possible on Microsoft standard software.
- The Council will maintain a Recovery Plan in case of loss, corruption or damage to ICT equipment, software or data.

### **3. Compliance with Legislation**

The Council's policy in respect of the requirements of the Data Protection Act 2018 is set out in its Information and Data Protection Policy.

Under the Computer Misuse Act 1990 (as amended by Part 5 of the Police and Justice Act 2006 and Part 2 of the Serious Crime Act 2015), the following are criminal offences, if undertaken intentionally:

- unauthorised access to a computer system or data;
- unauthorised access preparatory to another criminal action;
- unauthorised modification of a computer system or data;
- making, supplying or obtaining any articles for use in a malicious act using a computer;
- unauthorised acts causing serious damage,

All users should be made aware that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written "in-house", will be regarded as a breach of the Council policy and may be treated as gross misconduct. In some circumstances such a breach may also be a criminal offence.

It is an offence under the Copyright, Design and Patent Act 1988 to copy licensed software without the consent of the copyright owner. All copying is forbidden by the Act, unless it is in accordance with the terms and conditions of the respective licence or contract.

### **4. Security**

IT security is the protection of information systems from theft, damage interference or unauthorised use of the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services that they provide. It is the process of preventing and detecting unauthorised use of the computer system.

The Council will ensure that controls are put in place to provide confidentiality, integrity, and availability for all components of computer systems. These will include:

- Ensuring the secure location of equipment and documentation to help safeguard the Council's ICT assets. Portable equipment must be locked away when not in use and must not be removed from the premises without permission.
- Only persons authorised by the Town Clerk may use Council computer systems. The authority given to use a system will be sufficient but not excessive and users will be notified that the authority given to them must not be exceeded. Secure areas will be password protected.
- Developing operating procedures to control use of ICT equipment. Access to the Computers is subject to passwords. Levels of encryption will be maintained according to risk.
- Installing and keeping updated, reliable and reputable anti-virus software. (see below)
- Maintaining activated firewalls to act security guards between the internet and the computer network.

- Staying up to date with the latest software.
- Ensuring staff avoid clicking on email attachments unless they know the source.
- Changing passwords regularly, using a unique combination of numbers, letters and case types.
- Ensuring staff use the internet with caution and ignore pop-ups, drive-by downloads while surfing.
- Taking the time to research the basic aspects of computer security and educate ourselves on evolving cyber-threats.
- Performing daily full system scans and creating a periodic system backup schedule to ensure data is retrievable should something happen to a computer.
- Being satisfied that partner organisations or contractors who use their own systems have adequate security arrangements in place.

Further development of appropriate secure data storage, off site back up of data, and recovery plans will be a priority for review.

### **5. Virus Controls**

Viruses are undesirable pieces of computer code that can corrupt systems, equipment and data. They are a serious, increasing threat to the computer systems of the Council. All computers and servers will have loaded and operate the Council's standard virus detection software for scanning discs, memory sticks and fixed drives. Discs and memory sticks of unknown origin should not be used in the Council's computers.

No software should be loaded onto the Council's equipment without the permission of the Town Clerk.

If a virus is suspected, the equipment should be switched off and isolated until the virus can be eliminated.

### **6. Use of Computer Equipment**

1. Only authorised persons have use of computer equipment.
2. The use of new software must first be authorised by the Town Clerk or other nominated person before general use is permitted.
3. Only software authorised for business applications may be used.
4. Unauthorised copying or removal of computer equipment/software is not allowed.

### **7. Misuse**

This Policy applies to the activities which constitute unacceptable use of the network operated by the Council. The policy applies equally to employees, councillors, clients, visitors and others who may be allowed to use the facilities on a permanent or temporary basis. All misuse of the facilities is prohibited including specifically but not exclusively the following:

1. The creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material.
2. The creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
3. The creation or transmission of defamatory material.
4. The transmission of material in any way that infringes the copyright of another person.
5. The transmission of unsolicited commercial advertising material to networks belonging to other organisations.
6. Deliberate actions or activities with any of the following characteristics:
  - Wasting staff effort or networked resources
  - Corrupting or destroying another user's data
  - Violating the privacy of other users

- Disrupting the work of other users
- Other misuse of networked resources by the deliberate introduction of viruses
- Playing games during working hours
- Private use of the facilities without specific consent
- Altering the set up or operating parameters of any computer equipment without authority

## **8. Internet**

The internet is established as an important communications and information facility. At the Council these facilities are provided for use of staff and occasionally councillors to achieve Council objectives. Authorised persons are encouraged to make use of the Internet as part of their official and professional activities. Any use for unauthorised purposes outside of those permitted in this policy will be regarded as gross misconduct. If you are unsure whether use would be authorised, you must seek advice from the Town Clerk in advance. Visitors such as volunteers or contractors working with the Council may also be specifically authorised to use the Council's access to the internet, for the work they are doing for the Council.

You should not download files, including application and games that are not connected with your work for Flitwick Town Council. Any sites which require registration or payment for services must not be accessed without due authority. [See *Digital & Social Media Policy below*]

## **9. Use of Email**

The use of email is encouraged as its appropriate use facilitates efficiency. The email system is available for communication directly concerned with the legitimate business of the Council. An exchange of email correspondence requires the same professional standards as other forms of communication. You should not send or forward mail, which is defamatory or offensive for whatever reason, or is known to be factually incorrect or misleading.

In order to protect the Council from viruses, email attachments which might contain macros (word processor and spreadsheet files) or applications, should not be opened if they are from a sender whom you do not recognise, - simply delete.

Email addresses should be treated as confidential and care taken that private email addresses are not wrongly circulated. Email to multiple addresses outside of Councillors and the Clerk should be sent as blind copy, (bcc). [See *Social Media Policy*]

## **10. Social Media**

Social media is the term for online tools, websites and interactive media that enable users to interact with each other by sharing information, opinions, knowledge and interests. The term "social media" covers sites and applications including but not restricted to Facebook, Twitter, Flickr, LinkedIn, blogs, and any similar sites which develop after the creation of this policy. It also includes comments on online newspaper articles.

Social media can be a positive media, but it can lead to high emotions and online arguments. The additional risks to personal safety will be considered in safety risk assessments. (see *Health and Safety below*).

The Council has adopted a Social Media Policy which is included in this document as Appendix 4. For both councillors and officers it is to be considered in conjunction with their respective codes of conduct and associated protocols. It relates to all use of social media, whether inside or outside of official capacities. [See *Social Media*]

## **11. Health and Safety**

Computers are now a part of everyday life. If they are not used correctly, they can present hazards. Computers may be called Display Screen Equipment (DSE), Visual Display Units (VDU's) and the immediate environment where they are used i.e. desk/chair etc. is referred to as a workstation.

The Display Screen Equipment Regulations, 1992 regulate the use of computers at work and refer to the persons affected as "users". "Users" are persons who "habitually use VDU's as a significant part of their

normal work and regularly work on display screens for two/three hours each day or continuously for more than one-hour spells". The Regulations also apply to employees working at home.

The Council will ensure that a correct assessment of all workstations is undertaken to highlight any problems. In addition, there are risks which arise from possible arguments and harassment arising through social media.

## **12. Protocol for the use of Flitwick Town Council's Website.**

### **Background**

The Town Council operates two linked websites, the main Council one and The Rufus Centre. Both websites were developed and are hosted by an external provider. They will be further developed and made more interactive and have recognisable design links with a range of partner organisations.

Our website is the main media for the purpose of communicating information about the Town Council. The website and indeed email communications media may be used to:

- Post minutes and dates of meetings
- Advertise events and activities
- Publicise good news stories linked website or press page
- Vacancies
- Post and communicate information from partners i.e. Police, Library and Health etc.
- Announcing new information.
- Promulgate information required under the Transparency Code
- Give information on the Council, its policies and governance
- Post and communicate information from other Town related community groups, clubs, associations and bodies.
- Refer resident queries to the Town Clerk, other staff or councillors.

The Rufus Centre Website is intended to:

- Promote the conference, celebration and meeting facilities.
- Advertise regular and on- off events.
- Promote the café.
- Give information about community groups operating at the centre
- Advertise availability in rentable office space.

### **Future Additions**

The Council will regularly review the contents of its websites to ensure that it continuously improves the range and quality of current and historical data available.

### **Editorial Control**

The Town Clerk has been given editing rights for the Town Council site. The Town Clerk can add, delete and amend specified areas of information on the Town Council site. Quality is important to the image of the Council. Remember: anything that we publish on the web, we should be happy to see published in a local newspaper!

### **Editorial Content**

Information needs to be accurate and in accordance with Town Council Policy.

The Code of Recommended Practice on Local Authority Publicity 2015 must be taken into account when matters of publicity are concerned. Basically, we are allowed to publicise the contact details of individual councillors, positions they hold and can publicise individual proposals, decisions and recommendations but must keep information objective and not use Council funds to mount campaigns intended to persuade members of the public to hold a particular view on a question of policy or party politics. The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 require public sector websites to meet accessibility standards. They also apply to downloadable documents, mobile apps, intranets and extranets. The Council will publish an accessibility statement on its website and the Town Clerk will ensure compliance.

### **Updating the Site**

The site will be updated regularly. It is important that the site remains fresh, relevant and current.

## Web Links

We will place important links on our website to make it as easy as possible for visitors to find out information about the Town and its organisations. We will also approach other bodies for them to have links to our site- see Web links policy below.

### **13. Web Links Policy**

The website may include links to various outside bodies, including:

- Links to the websites of business who sponsor any Council event or facility,
- Links to external organisations providing a public service – e.g. Central Bedfordshire Council,
- Links to community partners

#### Criteria for outside link to Flitwick Town Council

From the adoption of this Policy, the following criteria will be used to decide what websites may be linked to the Flitwick Town Council website:

1. Other Council websites such as Central Bedfordshire Council, or other local councils in the greater Flitwick area.
2. Public service websites that provide information to the public, such as Police, Fire & Rescue Service, Safer Community Partnerships.
3. Tourism websites that provide information to people wishing to visit the local area
4. Specific business websites providing public information, at the discretion of the Council.
5. Contact for local churches
6. Links to websites of businesses who sponsor Council events or facilities.
7. Local History and Museum websites.
8. No individual businesses to be linked to the website, unless they are sponsors (as above).
9. Links to websites of community groups or clubs which serve the Town.
10. The Council to have the final decision as to whether a website meets the criteria set out in this Policy document.
11. The following Disclaimer to be used:  
“Our website contains links to these other sites to provide information and for the convenience of the public. Flitwick Town Council does not control these sites and so cannot guarantee that the information is up to date or correct. Flitwick Town Council does not endorse any of the content of any businesses linked to the website nor any advertising linked to these websites”.

### **14. Sharing Technology**

We will work and share technology with the principal council and other local bodies where appropriate, providing it takes forward the objectives of this policy.

#### Sharing information with and between Councillors

As much information as possible will be provided electronically to councillors. The Local Government (Electronic Communications) England Order 2015 has amended the Local Government Act 1972, Schedule 12 to allow the distribution of summonses, agendas and minutes by electronic means providing each councillor agrees.

Councillors historically print as necessary themselves, however it is at times necessary for councillors to print large documents and this facility is offered. Council specific email addresses and advice on the security of confidential information will be made available to councillors. The Council will in the future need to review these arrangements, along with the possibility of more useable technology provision.

## **Appendix 1.**

### **FLITWICK TOWN COUNCIL: DIGITAL AND SOCIAL MEDIA POLICY**

#### **Introduction**

The aim of this Policy is to set out a policy and code of practice to provide guidance to staff and town councillors in the use of online communications, collectively referred to as digital and social media. It is intended to supplement the main Digital and ICT Policy.

Digital and social media is a collective term used to describe methods of publishing on the internet. The policy covers all forms of digital media and social networking sites which include (but are not limited to):

#### Digital Media

- Town Council emails
- Town Council website

#### Social Media

Social Media applications include, but are not limited to:

- Social networking sites such as Facebook and LinkedIn
- Microblogging applications, for example Twitter
- Image and video sharing sites, such as YouTube and Flickr
- Blogs, for example Blogger
- Video streaming services, such as Twitch
- Discussion forums, such as Reddit
- Instant Messaging services, such as Messenger, WhatsApp and Skype
- Reference sources such as Wikipedia

#### **Who does it apply to?**

The principles of the Policy apply to Town Councillors, all Council Staff and any volunteers or contractors working with the Council. It is also intended for guidance for others communicating with the Town Council.

#### **The scope of the policy**

- All employees and elected members are expected to comply with this policy at all times to protect the privacy, confidentiality, and interests of the Council.
- Breach of this policy by employees may be dealt with under the Council's Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.
- Breach of this policy by elected members may be a breach of the Councillor Code of Conduct.

#### **Responsibility for implementation of the policy**

- The Council has overall responsibility for the effective operation of this policy.
- The Town Clerk is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to our work.
- All employees and elected members should ensure that they take the time to read and understand this policy. Any breach of this policy should be reported to the Town Clerk or Chairman of Audit Sub-Committee.
- The Corporate Services Committee may include the monitoring of the application of this policy in their audit programme.

#### **Email and Telephones**

This part of the policy sets out the restrictive use of the Town Council's electronic equipment, namely, computers and telephones.

Emails will be used to distribute information of council business.

Communications via email internet usage undertaken in the name of the Council or on Council systems carry inherent risks such as:

- Potential defamation
- Spreading of viruses, including Trojans which can steal data
- Breach of confidentiality
- Accepting files from sources in online chat rooms which could bypass firewalls or email filters



- Breach of contract
- Breach of copyright
- Breach of data protection legislation
- Breach of privacy and unlawful discrimination

The Council provides telephones, email and internet access solely for the purposes required for the performance and fulfilment of job responsibilities. Occasional and reasonable personal use of the Council's telephone, internet and email service is permitted, provided that it does not interfere with work performance or security.

### **Monitoring and Privacy Issues**

The Town Council reserves the right to monitor telephone, email and internet usage in accordance with the law, in particular the latest Data Protection Act 2018, General Data Protection Regulations and the Human Rights Act 1998.

Internet and email usage may be monitored from time to time in order to identify potential breaches of this Policy. This may lead to formal disciplinary action. Employees should note that serious breaches may result in dismissal for gross misconduct. However, the Town Council is subject to Article 8 of the Human Rights Act, and this means that the Council will respect employees' private and family life.

### **Email etiquette**

All employees must follow the procedure outlined below when sending and receiving emails on behalf of the Town Council:

- Only agreed email signatures may be used
- All messages must use appropriate business language
- A waiver clause will be included at the end of each email message
- The circulating of offensive, indecent or obscene material or anything which breaches the Equal Opportunities Policy is strictly prohibited.
- Confidential material should not be disclosed unless it needs to be forwarded to a particular person and is authorised.
- Only attachments from a trusted source may be downloaded
- Ensure that the address of the recipient is correct before sending emails
- Ensure that a 'reply to all' is appropriate
- Ensure that essential files are saved before deleting the message in which they were received.

Individual Town councillors must use their town council email address for their role as a councillor and not their private email. Councillors are personally responsible for any online activity conducted via their council e-mail address. They must adhere to the Members' Code of Conduct, and any related protocols.

### **Telephone etiquette**

All employees must follow the procedure outlined below when using the Council's telephone:

- Answer all calls by stating the name of the Town Council and their own name
- Be polite at all times
- Do not be rude or abrupt to callers, even if they are.
- Do not use offensive language
- Do not swear
- Check the telephone frequently for messages from callers and respond in a timely manner

Employees may make and receive personal calls as long as they are brief and infrequent. This applies to calls on the Council's land line or employees' personal mobile phones.

### **Unacceptable behaviour on the internet**

Below are examples of what the Town Council deems to be unacceptable use or behaviour by employees:

- Allowing non-authorised users to access the internet using employees log in or while logged on.
- Visiting internet sites that contain obscene, hateful, pornographic or other illegal or unsavoury material.
- Passing on such material to colleagues or external people.
- Using the computer to perpetrate any form of fraud or software, film or music piracy.
- Using the internet to send offensive or harassing material to other users.

- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Publishing defamatory and/or knowingly false material about the Council, its employees, members, colleagues and/or customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of malicious software into the corporate network.
- Gambling on-line.
- Disclosure of any confidential corporate information without express consent.
- Any other area that the Council reasonably believes may cause problems.
- Publishing personal opinion which is contrary to Council policy, or which is about matters which would not be considered part of the employee's remit.

## **Website**

The use of digital and social media does not replace existing forms of communication. The main media for the purpose of communicating information about the Town Council is our website. The website and other forms of social media will be used to enhance communication. Therefore, existing means of communication should continue with social media being an additional option, but one of growing importance.

## **Social Media**

This section of the policy is intended to help employees and elected members make appropriate decisions about the use of social media such as social networking websites, forums, message boards, blogs or comments on web-articles, such as Twitter, Facebook and LinkedIn. (see main policy above)

It outlines the standards the Council requires employees and elected members to observe when using social media, the circumstances in which your use of social media will be monitored and the action that will be taken in respect of breaches of this policy.

## **Use of Digital and Social Media channels owned by Flitwick Town Council**

The Council have appointed SMAT as moderator for Council-owned digital and social channels. SMAT will be responsible for overseeing and monitoring of the content, ensuring it complies with the Digital and Social Media Policy. The Town Clerk will have authority to remove any posts made by third parties from our social media pages which are deemed to be of a defamatory, offensive or libellous in nature. Such posts will also be reported to the Hosts (i.e. Facebook).

The Corporate Services Committee will, as part of their audit programme, also monitor digital and social media channels.

Social media channels, such as Facebook, will be used to share the website information above with links referring to the Flitwick Town Council website.

All social media sites in use should be checked and updated on a regular basis and ensure that the security settings are in place.

Councillors may discuss items which they believe should be included on the Council's social media channels with SMAT. They will have no direct responsibility for such postings.

Not all communication requires a response. There will not be immediate responses to communications that may be discussed by the Council or a committee. Communications should be acknowledged.

- The Town Clerk will be responsible for all final published responses.
- If a matter needs further consideration it may be raised at either the open forum or as a full agenda item for consideration by a quorum of Councillors. Again, the poster shall be informed via the page or direct message that this is the case.

## **Basics on communicating with residents, colleagues and officers**

- Confidential information should generally not be disclosed
- Bear in mind obligations under data protections rules

- Consider carefully forwarding or sharing third party communication, in case it could be affected by copyright rules, could be considered defamatory material or may be inaccurate.

### **Personal Guidance for Councillors using Digital channels and Social Media**

The Council's social media channels do not currently have pages for individual councillors and therefore councillors generally post through their own social media accounts. Councillors may respond to a post on the Council's social media channels but are perhaps better to allow officers to respond to third party postings.

Social media can be very useful in getting feedback on proposals and communicating information about Councillors' activities.

Social important media is always on, so consider setting personal limits and establishing your own routine.

Councillors' are subject to the council's code of conduct when using social media

Some Councillors' choose to have separate social media profiles for personal and council use. It is important to keep in mind, however, that even the strictest privacy settings are no guarantee for posts or actions to remain private. As a rule of thumb, never post anything online you would not be comfortable saying or sharing in a public meeting.

It is that Councillors' set out clearly in their communications whether it is sent in their Councillor role or in a private capacity.

Councillors' are personally responsible for the content they publish on any form of social media. Publishing or allowing to be published (in the form of a comment) an untrue statement about a person which is damaging to their reputation may incur a defamation action for which you will be personally liable. The same applies if you pass on any similar untrue statements you receive.

Social media sites are in the public domain and it is important to ensure you are confident of the nature of the information you publish. Once published, content is almost impossible to control and may be manipulated without your consent, used in different contexts, or further distributed.

Consider your personal safety and security and incorporate it into planning any public duties or interaction, in association with the Town Clerk. Much personal safety is common sense, but it is useful to remind yourself of the advice.

When participating in any online communication;

- Be responsible and respectful; be direct, informative, brief and transparent.
- Always disclose your identity and affiliation to the Town Council. Never make false or misleading statements.
- Be mindful of the information you post and do not present yourself in a way that might cause embarrassment.
- Personal opinions must not be published as being representative of the Council, bring the Council into disrepute or act contrary to the Council's Code of Conduct, associated protocols or any other Policies. Where Councillors identify themselves as such on social media channels, it is recommended that, in the personal biography information on Twitter and similar channels, Councillors state "Opinions I express here are my personal views and not those of Flitwick Town Council"
- Keep the tone of your comments factual and informative, never condescending or "loud." Use sentence case format, not capital letters, or write in red to emphasis points.
- Refrain from posting controversial or potentially inflammatory remarks. Language that may be deemed as offensive relating in particular to race, sexuality, disability, gender, age or religion or belief should not be published on any social media site.
- Keep arguments offline.
- Don't write in haste. Avoid writing when you are angry, upset, or tired.
- Avoid personal attacks, online fights and hostile communications.
- Never use an individual's name unless you have written permission to do so.

- Permission to publish photographs or videos on social media sites should be sought from the persons or organisations in the video or photograph before being uploaded. It is advised that if you wish to distribute an image or video from an external source, that this is done by sharing or linking to the external source's original post, image or video.
- Respect the privacy of other councillors and residents.
- Do not post any information or conduct any online activity that may violate laws or regulations,
- Be careful. Some people say things via social media that they probably would not say in person, and they can post false information, insults or messages that you would not want to be associated with you. These can multiply and be shared quite rapidly. Councillors' and in particular female Councillors' are unfortunately increasingly the subject of online abuse, bullying and harassment on social media.
- Sometimes, it is better to try to switch ongoing dialogue to another media such as email.
- If you feel unable to answer a post for example of a contentious nature this shall be referred to the SMAT. The poster will be informed by way of response to this fact and also be invited to correspond with the Town Clerk directly.
- Some communication from residents and other third parties may be required to be discussed at a Town Council meeting. When this is necessary the item will be placed on the next available agenda. Any response will then be included in the minutes of the meeting.

The Council will support Councillors' in their use of social media. If you need advice or if things go wrong, please contact the Town Clerk.

### **Guidance to members of staff**

Whilst an officer's postings on the Council's social media sites will be controlled, they are expected to take account of the views of the public, respond to requests for a service and deal with complaints in the normal manner.

Staff may also have personal social media accounts, the contents of which are their own affair. They are however, expected not to comment on the business of the Council or on matters in the Town which the Council are involved in, or respond to third party posts on such matters. Any member of staff making detrimental comments about Flitwick Town Council or its Councillors, will immediately be subject too disciplinary action.

The guidance given to councillors, largely applies to employees.