FLITWICK TOWN COUNCIL

DIGITAL & ICT POLICY

Contents

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: Digital & 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 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.
- 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 Instagram,, 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 website www.flitwick.govuk and The Rufus Centre – www,therufuscentre.co.uk. Both websites are hosted by an external provider.

Our website is one of the main platforms for communicating information about the Town Council. The website may be used to:

- Post agendas, supporting papers, minutes and dates of meetings
- Advertise events and activities
- Publicise good news stories including press release page
- Vacancies
- Post and communicate information from partners i.e. Police, Library and Health etc.
- Announce new information.
- Promulgate information required under the Transparency Code
- Give information on the Council, Members, its policies and governance
- Post and communicate information from other Town related community groups, clubs, associations and bodies.
- Promote Flitwick businesses through the Business Directory
- 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 one- off events including third party events held at The Rufus Centre
- Provide booking link to Ticketsolve booking platform for FTC and Rufus events.
- Promote the Rendezvous Café.
- Give information about community groups operating at the centre
- Advertise availability of rentable office space.
- Provide links to tenants based at centre.

Future Additions

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

Editorial Control

Officers have been given editing rights for the Town Council site andcan add, delete and amend specified areas of information on the Town Council site. Quality is important to the image of the Council.

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. Links to websites of community groups or clubs which serve the Town.
9. The Council to have the final decision as to whether a website meets the criteria set out in this Policy document.
10. 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:
REMOVEABLE MEDIA POLICY

1. Policy Statement

Flitwick Town Council will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business.

2. Purpose

This document states the Removable Media policy for Flitwick Town Council. The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of Flitwick Town Councils Council's computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Protected and Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

3. Scope

This policy applies to all Members, Committees, Services, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Flitwick Town Council information, information systems or IT equipment and intends to store any information on removable media devices.

4. Definition

This policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the Council to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following:

- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras. .
- Audio Tapes (including Dictaphones and Answering Machines).

5. Risks

Flitwick Town Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business. Information is used throughout the Council and sometimes shared with external organisations and applicants.

Securing **PROTECTED or RESTRICTED** data is of paramount importance – particularly in relation to the Council's need to protect data in line with the requirements of the Data Protection Act 1998 & 2018. Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the Council.
It is therefore essential for the continued operation of the Council that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the Council's needs.

This policy aims to mitigate the following risks:

- Disclosure of **PROTECTED** and **RESTRICTED** information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of Council networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6. Applying the Policy

6.1. Restricted Access to Removable Media

It is Flitwick Town Council policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to the Town Clerk for **Approval.**

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

6.2. Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by the Council's outsourced IT provider. Non-council owned removable media devices must not be used to store any information used to conduct official Council business and must not be used with any Council owned or leased IT equipment.

The only equipment and media that should be used to connect to Council equipment or the Council network is equipment and media that has been purchased by the Council and approved or has been sanctioned for use by the Council.

6.3. Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Therefore, removable media should not be the only place where data obtained for a council purpose is held.
Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another

networked computer or system.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all **PROTECTED or RESTRICTED** data held must be encrypted.

Users should be aware that the Council will audit / log the transfer of data files to and from all removable media devices and Council-owned IT equipment.

6.4. Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to the Town Clerk.

It is the duty of all Members to report any actual or suspected breaches in information security to the Chairman of the Council.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident.

6.5. Third Party Access to Council Information

No third party (external contractors, partners, agents, the public or non-employee parties) may receive data or extract information from the Council's network, information stores or IT equipment without explicit agreement from the Council's outsourced IT provider acting on behalf of Flitwick Town Council.

Should third parties be allowed access to Council information then all the considerations of this policy apply to their storing and transferring of the data.

6.6. Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the Council's outsourced IT provider should removable media be damaged.

Virus and malware checking software approved by the Council's outsourced IT provider must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by two functionally different virus checking software products, before the media is loaded on to the receiving machine.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the Council, other organisations or individuals from the data being lost whilst in transit or storage.

6.7. Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the Council or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to the Council's outsourced IT provider for secure disposal.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the Council's outsourced IT provider.

6.8. User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives).

- Any removable media device used in connection with Council equipment or the network or to hold information used to conduct official Council business must only be purchased and installed by the Council's outsourced IT provider. Any removable media device that has not been supplied by IT must not be used.

- All data stored on removable media devices must be encrypted where possible.

- Virus and malware checking software must be used when the removable media device is connected to a machine.

- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.

- Removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.

- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

For advice or assistance on how to securely use removable media devices, please contact the Council's outsourced IT provider.

7. Policy Compliance

If any user is found to have breached this policy, they may be subject to Flitwick Town Council's disciplinary procedure.
If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

APPENDIX 2

FLITWICK TOWN COUNCIL:
INTERNET ACCEPTABLE USAGE POLICY

1. Policy Statement

Flitwick Town Council will ensure all users of Council provided internet facilities are aware of the acceptable use of such facilities.

2. Purpose

This policy document tells you how you should use your Council Internet facility. It outlines your personal responsibilities and informs what you must and must not do.

The Internet facility is made available for the business purposes of the Council. A certain amount of personal use is permitted in accordance with the statements contained within this Policy.

It is recognised that it is impossible to define precise rules covering all Internet activities available and adherence should be undertaken within the spirit of the policy to ensure productive use of the facility is made.

3. Scope

This Internet Acceptable Usage Policy applies to, but is not limited to, all Flitwick Town Council Members, Committees, Services, Partners, Employees of the Council, contractual third parties and agents of the Council who access the Council's Internet service and IT equipment.

4. Definition

This Internet Acceptable Usage Policy should be applied at all times whenever using the Council provided Internet facility. This includes access via any access device including a desktop computer, council laptop, or a smartphone device.

5. Risks

Flitwick Town Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- Viruses, malware etc.
- Increased risk of data loss and corresponding fines
- Inappropriate access to and unacceptable use of the Council's network, software, facilities And documents.
- Inadequate destruction of data
- The non-reporting of information security incidents
- Inconsistency in how users deal with 'secure' documents
- The impact of insufficient training for users
- The sharing of passwords
- Incorrect or inappropriate classification of documents
- Risk of reputation damage and further loss in public confidence
- Operational difficulties providing services
- Inappropriate sharing of personal data in breach of the Data Protection Act 1998 & 2018.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6. Applying the Policy

6.1. What is the purpose of providing the Internet service?

The Internet service is primarily provided to give Council employees and Members:

- Access to information that is pertinent to fulfilling the Council's business obligations.
- The capability to post updates to Council owned and/or maintained web sites
- An electronic commerce facility.
- An ability to engage online with our customers.

6.2. What you should use your Council Internet account for

Your Council Internet account should be used in accordance with this policy to access anything in pursuance of your work including:

- Access to and/or provision of information.
- Research.
- Accessing browser-based IT applications.

6.3. Personal use of the Council's Internet service

At the discretion of your line manager, and provided it does not interfere with your work, the Council permits the use of the Internet facilities for non-business research or browsing during unpaid mealtimes or unpaid before/after flexitime/normal working hours.

Personal use of the Internet is subject to management discretion and the following conditions:

- To investigate or detect the unauthorised use of the systems, e.g. that the policy is being observed, that no discriminatory or offensive content appears in emails, etc.
- That personal use does not impinge on the member of staff's work or that of other staff;
- That personal use takes place outside of normal working hours and that the time is not included in the calculation of daily hours; and
- That personal use is not connected to any business or profit-making venture.

In addition to these general restrictions noted above, the Council specifically excludes the following uses of the Internet:

- To view content of an obscene or discriminatory nature, or content that is in violation of UK legislation.
- To download unofficial software for use on Council equipment.
- To reveal confidential information.
- To spread or publish any political, with the exception of recognised Trade Union Activity, or threatening views or content that could cause unrest. To search for personal information using the business email address.

6.4. Use of Social media

- You must not access social networking sites for personal use during working hours. Access to the Web using the Councils IT systems is restricted to lunch breaks and before and after the working day, unless specific permission is granted by your manager.

- You may not use Facebook page for personal blogs unless the use is in line with the Town Councils Social Media Policy.

- Employees must not give information on a social networking site which is confidential to the Council, its suppliers or customers.

- Employees must refrain from making reference on social networking sites to the Council, its employees, its customers and its suppliers.

- Employees must not post entries on Facebook or a social networking site which are derogatory, defamatory, discriminatory or offensive in any way, or which could bring the Council into disrepute.

- Employees should be aware that blogs may create documents which the courts can order to be disclosed for use in litigation. Consequently, employees will be assumed to have written any contentious items unless they can prove definitively that they have not done so.

- The Council will monitor its IT systems as is deemed necessary in order to prevent inappropriate usage Monitoring use of social media during work time.

- The Council reserves the right to monitor employees Internet usage, the Council considers that valid reasons for checking and employees Internet usage include suspicions that the employee has been spending an excessive amount of time using social media websites for non-work-related activity; or acted in a way that is in breach of the rules set out in this policy

- The Council reserves the right to retain information that it has gathered on employees use of the Internet for a period of one year.

- Access to particular social media sites may be withdrawn in any case of misuse.

Note:

Access to on-line games and the use of social chat rooms or forums will be reviewed and may be blocked for business reasons e.g. streaming media, impact on services, or due to content being downloaded.

Please refer to the Town Council Social Media Policy.

Staff purchase personal items at their own risk. The Council is not responsible for any personal transactions you enter into. You must accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from your transaction – for example in relation to payment for the items or any personal injury or damage to property they might cause.

If you are in any doubt about how you may make personal use of the Council's Internet service, you are advised to discuss this with your Manager.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Flitwick Town Council and may be accessed at any time by the Council to ensure compliance with all its statutory, regulatory and internal policy requirements.

6.5. Internet account management, security and monitoring

The Council will provide a secure logon-id and password facility for the network which will include access to the internet. The Council's outsourced IT provider is responsible for the technical management of this account.

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted by lack of capacity.

• The filtering system monitors and records all access for reports that are produced for line managers and auditors.

6.6. Things you must not do

Access to the following categories of websites is currently blocked using the Websense URL filtering system.
Please note that this is not exhaustive and will be updated as appropriate:

• Illegal.
• Pornographic.
• Violence.
• Hate and discrimination.
• Offensive.
• Weapons.
• Hacking.
• Gambling.
• Dating.
• Radio stations.
• Games.

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must not use your Internet account to:

Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.

Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.

Subscribe to, enter or utilise real time chat facilities such as chat rooms.

Subscribe to, enter or use online gaming or betting sites.

Subscribe to or enter "money making" sites or enter or use "money making" programs.

Run a private business.

Download any software that does not comply with the Council's Software Policy. The above list gives examples of "unsuitable" usage but is neither exclusive nor exhaustive. "Unsuitable" material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.

6.7. Your responsibilities

It is your responsibility to:

Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.

Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

Know that you may only use the Council's Internet facility within the terms described herein.

Read and abide by the following related policies: Email Acceptable Use Policy. Software Policy.IT Access Policy. Removable Media Policy.

6.8. Line Manager's responsibilities

It is the responsibility of Line Managers to ensure that the use of the Internet facility:

Within an employee work time is relevant to and appropriate to the Council's business and within the context of the user's responsibilities.
Within an employee's own time is subject to the rules contained within this document.

APPENDIX 3

FLITWICK TOWN COUNCIL:
IT ACCESS POLICY

1. Policy Statement

Flitwick Town Council will establish specific requirements for protecting information and information systems against unauthorised access.

Flitwick Town Council will effectively communicate the need for information and information system access control.

2. Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, asset of Flitwick Town Council which must be managed with care. All information has a value to the Council. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3. Scope

This policy applies to all Flitwick Town Council Members, Committees, Services, Partners, Employees of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Council with any form of access to Flitwick Town Council's information and information systems.

4. Definition

Access control rules and procedures are required to regulate who can access Flitwick Town Council information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Flitwick Town Council information in any format, and on any device.

5. Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6. Applying the Policy - Passwords

6.1. Choosing Passwords

Passwords are the first line of defence for our ICT system and together with the user ID help to establish that people are who they claim to be.
A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.
The Council will enforce Multi Factor Authentication, (MFA) when accessing FTC accounts.

6.1.1. Weak and strong passwords

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

• At least seven characters.
• Contain a mix of alpha and numeric, with at least one digit
• Cannot have two consecutive characters which are the same
• More complex than a single word (such passwords are easier for hackers to crack).

The Government advises using Environ passwords with the following format: consonant, vowel, consonant, consonant, vowel, consonant, number, number. An example for illustration purposes is provided below:

• pinray45

6.2. Protecting Passwords

It is of utmost importance that the password remains protected. The following guidelines must always be adhered to:

• Never reveal your passwords to anyone.
• Never use the 'remember password' function.
• Never write your passwords down or store them where they are open to theft.
• Never store your passwords in a computer system without encryption.
• Do not use any part of your username within the password.
• Do not use the same password to access different Flitwick Town Council systems.
• Do not use the same password for systems inside and outside of work.

6.3. Changing Passwords

All user-level passwords must generally be changed every 60 days, unless there are special cases that justify this being different, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect,

that your password has become known to someone else, you must change it immediately and report your concern. Users must not reuse the same password within 20 password changes.

6.4. System Administration Standards

The password administration process for individual Flitwick Town Council systems is well-documented and available to designated individuals.

All Flitwick Town Council IT systems use ‘Active Directory’ and will be configured to enforce the following:

• Authentication of individual users, not groups of users - i.e. no generic accounts, Multi Factor Authentication, (MFA) will be used when accessing FTC accounts.
• Protection with regards to the retrieval of passwords and security details.
• System access monitoring and logging - at a user level.
• Role management so that functions can be performed without sharing passwords.
• Password admin processes must be properly controlled, secure and auditable.

7. Applying the Policy – Employee Access

7.1. User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by Flitwick Town Council. Each user must be allocated access rights and permissions to computer systems and data that:

• Are commensurate with the tasks they are expected to perform.
• Have a unique login that is not shared with or disclosed to any other user.
• Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

7.2. User Registration

A request for access to the Council's computer systems must first be submitted to the Town Clerk / Deputy Town Clerk, access must only be gained if approval has been given.

When an employee leaves the Council, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of their Town Clerk / Deputy Town Clerk to request the suspension of the access rights via the Council's outsourced IT provider.

7.3. User Responsibilities

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:

• Following the Password Policy Statements outlined above in Section 6.
• Ensuring that any PC they are using that is left unattended is locked or logged out.
• Leaving nothing on display that may contain access information such as login names and passwords.

7.4. Network Access Control

Only Council owned - equipment connected to wired network connections and the Corporate Wi-Fi SSID. All personal devices should be connected to the guest Wi-Fi network. The normal operation of the network must not be interfered with, approval must be obtained before connecting any equipment to the Council's network.

7.5. User Authentication for External Connections

Where remote access to the Flitwick Town Council network is required, an application must

be made via the Town Clerk and the Council's outsourced IT provider.

7.6. Supplier's Remote Access to the Council Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission.
Partners or 3rd party suppliers must contact the Town Clerk and the outsourced IT provider before connecting to the Flitwick Town Council network and a log of activity must be maintained. Third party access will be supervised.
Remote access software must be disabled when not in use.

7.7. Operating System Access Control

Access to operating systems is controlled by a secure login process.
The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorised users are allowed.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

7.8. Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The owner' of the software application is responsible for granting access to the information within the system.

- Be compliant with the Password section (section 6) above.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

8. Policy Compliance

If any user is found to have breached this policy, they may be subject to Flitwick Town Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Appendix 4.

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, Tik Tok, Pininterest
- 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 HR Committee.

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 and Facebook pages. The website and other forms of social media will be used to enhance communication.

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 Facebook, Instagram 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 the Senior Management Team (SMT) as moderator for Council-owned digital and social channels. SMT 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).

Social media channels, such as Facebook and Instagram, will be used to share news and information referring to the FTC or The Rufus Centre website with links where applicable.

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 SMT. 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 and/or Communications & Marketing Manager 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' 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 SMT. 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 Councilors' 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.