Buckinghamshire Council

Acceptable Use Policy	**Approved By: Chief Executive Officer**	31 January 2020	
	Date Created:	22 January 2020	
	Previous Version:		
	Next Review Date:	31 January 2021	
	Policy Number:	1	
	Department:	ICT	

PURPOSE

The purpose of the Acceptable Use Policy is to ensure that all computer systems and networks owned or managed by Buckinghamshire Council are operated in an effective, safe, ethical and lawful manner and it is the responsibility of every computer user to know these requirements and to comply with them.

POLICY

Access Control

1.1 **Users are only permitted to access information, applications and systems that they have been allocated access rights for. Rights are granted on the basis of business need and documented such that it defines the rules and rights for individuals or groups. Any other access is considered unauthorised and is in breach of this requirement.**

Explanation
Users are not permitted to access any information systems resource (computing device, network, information repository) owned or managed by Buckinghamshire Council that they are not authorised to access. The casual browsing of network shares looking for interesting files or programs is not permitted. Using another user's ID for access and/or copying data or information into areas where the user has legitimate access in order to gain unauthorised access to it is considered a serious breach of security.

1.2 **Mobile phones, tablets, portable computers, laptops, USB devices or any other device must not be connected to Buckinghamshire Council's internal computer systems or networks unless the device has been approved for use by the IT Operations Manager.**

Users should not access systems that contain personally identifiable information (PII) from mobile devices or save any PII information onto USB devices etc unless approval has been given by the IT Operations Manager.

Explanation
Connecting portable devices to computer systems and networks may expose the Council to unauthorised information disclosure and introduce malicious code. This control is required because these devices often have little protection against security threats.

Electronic calendars and address books are widely used and many devices provide internet browsing and access to email and internal corporate applications. Buckinghamshire Council must be able to determine the boundaries of its own information systems by mandating the appropriate controls.

1.3 Damaging, altering, or disrupting the operations of the computer systems and networks owned or managed by Buckinghamshire Council is not permitted. Users must not carry out any activity with the intention of capturing or obtaining passwords, encryption keys, or anything that could facilitate unauthorised access by themselves or anyone else.

Explanation
This control is needed to prevent users from carrying out hacking or cracking activities including theft or alteration of data or denial of service. It is intended to cover activities such as social engineering (where someone pretends to be someone else)and the use of keyword loggers, data sniffers or any other technique that records passwords using various methods of interception.

The scope is also intended to include smart cards, dynamic password tokens and any other means of achieving authentication as well as just user names and passwords.

Anti-Virus

2.1 Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise affect the performance of, or access to any Buckinghamshire Council computer system or network.

Explanation
Code designed to disrupt or replicate in networks is difficult to contain and isolate and the safest approach is to prohibit users from getting involved with them. This requirement also applies to computer programs which allow users to build viruses using tools downloaded from the internet. These activities will be considered misconduct and may result in actions up to and including dismissal being taken under the Council's Conduct and Discipline Procedures.

2.2 Users must not open files or click on links in attachments, emails or social media if the source is unknown, suspicious or untrustworthy.

Explanation
If a user suspects there may be something odd about the file, message or link, it is important that it is never opened as this can activate the threat and cause the computer systems and network to become infected. Users must report their suspicions to the Service Desk who will act accordingly.

Communication And Mobile Devices

3.1 **Mobile devices and communication systems supplied by the Council are provided to facilitate business activities. Reasonable and appropriate personal use is permitted as follows:-**

- **Minimal calls and text messages**
- **The data plan must not be exceeded due to personal use**
- **Personal use must not cause the Council to incur any additional costs or impact staff productivity**

Usage of devices and systems is monitored. Personal use may be required to be reimbursed.

A phone supplied by Buckinghamshire Council may not be used in connection with any personal commercial business activities. The number may not be published in any publication or business card that is not related to the Council's business.

Explanation
The intention of this requirement is to clarify what is acceptable behaviour regarding the personal use of communication systems and mobile devices supplied by the Council and disallows the use of these devices for personal chatting, randomly browsing the internet, downloading large amounts of data and any other activity which may incur a cost against Buckinghamshire Council.

3.2 **Mobile devices and communication systems owned or managed by Buckinghamshire Council are to be used in an effective, safe, ethical and lawful manner. Use will be monitored and misuse will be handled in accordance with Buckinghamshire Council's Conduct and Disciplinary Procedures.**

Explanation
Mobile phones and communications systems are put in place to support the business and must not be used for illegal or unethical purposes in any circumstances. Illegal or damaging actions whether performed knowingly or unknowingly may bring Buckinghamshire Council into disrepute and therefore misuse may be treated as misconduct and managed under the Council’s Conduct and Discipline Procedures.

3.3 **Users of Buckinghamshire Council's mobile phones and communication systems must not engage in any activity which violates or infringes the rights of others or which a reasonable person would consider to be abusive, profane, offensive or defamatory.**

Explanation
This requirement protects against breaches of human rights legislation. Using the Council's equipment or systems to harass, discriminate against or victimise another person is considered misconduct and will be handled in accordance withBuckinghamshire Council's Conduct and Disciplinary Procedures. If appropriate, the matter may be handed over to the police. These types of activities create a hostile work environment and will not be permitted.

3.4 **Communications equipment supplied by Buckinghamshire Council must not be altered or added to in any way including:-**

- **unauthorised upgrades**

- **addition of components**
- **removal of components - including transferring a Council SIM card to a personal phone**
- **altering configuration or security settings**
- **installation of non-approved applications**
- **jailbreaking the device**

All devices will be centrally managed and any changes or maintenance carried out by the Service Desk or designated agent.

Explanation
Users must not alter equipment provided by the Council as errors could cause the device to malfunction and void manufacturers' warranties. A user may inadvertently or deliberately bypass security measures, cause confidential or sensitive information to be lost or disclosed and provide an opportunity for hackers to compromise the machine.

In addition, this requirement protects against the removal of internal components like memory chips and helps to ensure the equipment issued to a user is the same equipment that will be returned when the user no longer requires it. This is important where equipment is leased.

3.5 Users of mobile devices must ensure that the device is protected by a PIN number, password, biometric authentication and auto-lock. Voice authentication (if used), must be coupled with password or PIN authentication.

Explanation
As mobile devices become more widely used to access and store important corporate information such as customer lists, email, diaries and documents users must ensure that they are protected from unauthorised access. For example, hundreds of mobile devices are left in public places every year and many of these have business information stored on them and have unrestricted remote access into corporate networks.

These devices are just another device on the network and because they operate from remote locations they effectively extend the Council's corporate network boundary. Buckinghamshire Council must be able to protect it's network perimeter from unauthorised access and therefore appropriate password and authentication rules must be applied to these devices.

3.6 Buckinghamshire Council maintains the right to conduct inspections of any mobile phone or other mobile device that it owns or manages without prior notice to the user or custodian. The device must be returned to the Service Desk upon request for maintenance and when the user ceases to provide services to Buckinghamshire Council.

Explanation
No matter where it is located, the Council reserves the right to conduct an inspection of the device or monitor traffic on any of its networks. This requirement ensures that corporate assets are protected firstly by confirming the existence of the equipment and secondly, that users are complying with health and safety, security and acceptable use Policies and Guidelines.

3.7 Users should not lend any devices allocated to them for business activities to others external to the Council including friends and family.

Explanation
Any equipment and allocated to Users is for their sole use. A wide variety of controls such as PIN numbers and passwords, encryption measures and other user settings are set up for a specific individual given that individual's job duties and the "need to know" principle.

Allowing another person to access that device (except for maintenance which is unavoidable), may allow the other person to access corporate information. Mobile phone calls cost money so care must be taken to ensure that they are used mainly for business purposes and not as a personal phone.

This requirement also gives users a definitive reason for not lending out equipment that has been allocated to them by saying it is against the Council's rules.

3.8 Unless approved, users must not return calls, text messages, respond to pager calls or subscribe to paid services where:-

- **the return number is a premium rate number**
- **charges beyond those for normal calls can be incurred (e.g. long distance calls)**
- **the recipient is a competition, gambling or advertising entity**
- **charges will be reversed back to the Council**

Any costs incurred relating to the above will be the responsibility of the staff member.

Explanation
These services are usually non business related so are not necessary and incur a fixed cost which is more than a normal call or text. This requirement is necessary to prevent non-business related use escalating out of control. Where these types of services are used the user will be responsible for the costs.

3.9 With the exception of applications supplied by Buckinghamshire Council from an approved online application store, games, freeware, shareware, movie clips or music may not be downloaded onto any Council mobile device unless its use is legal and it is specifically required for business purposes. Movie clips taken with the device for work purposes are exempt from this requirement.

Users should contact the Service Desk if they require a non-approved application on their device.

Explanation
Games may be infected with computer viruses, trojan or other malware and distract employees from their assigned duties. Games are often copied illegally and sent on to friends and may subject Buckinghamshire Council to liability for unauthorised software copying. This requirement includes the downloading of ringtones, especially if they incur a cost, and movie clips or music which are often pirated.

3.10 Personally owned communication devices must not be connected to or synchronised with Buckinghamshire Council's computer systems or networks unless approved and the device owner agrees to the security requirements regarding the management of the device. BYOD security requirements include but not limited to:-

- **Agreement that the corporate applications and data will be managed by Buckinghamshire Council**
- **Agreement for the Council security profile to be applied to the device**

Explanation
Buckinghamshire Council must be able to protect its ICT resources and in order to do this it must be able to apply specific security settings and limit the functionality of the device. One of the biggest threats to corporate ICT security is the portable device which is periodically connected to the corporate network as this may potentially introduce viruses and other malware and aid information leakage.

Portable devices owned personally by staff or contractors may not always have the tightest security as this often impacts on functionality, e.g. password or pin protection. The Council must be able to ensure that every device connected to the computer system and/or network has the same configuration and security settings applied and therefore the level of risk is mitigated.

3.11 Voice and video systems are not to be used for any of the following:-

- **commercial announcements**
- **advertising material**
- **sexually explicit or sexually oriented material**
- **hate based material**
- **hacker related material**
- **transferring of files**

All inbound and outbound communication must be channelled through corporate systems and accounts.

Explanation
Voice and video communication systems are provided to facilitate the Council's business. Personal use of corporate accounts is not permitted. Misuse will be handled in accordance with the ~EntityShortNames~'s Disciplinary Policy and Procedure.

Computer Systems And Equipment Use

4.1 Users of computer systems or networks owned or managed by Buckinghamshire Council shall not use these systems to engage in any activity which causes, or could be construed as causing, any form of harassment, discrimination or victimisation on the basis of:-

- **race**
- **religious belief or activity**
- **sex**
- **age**
- **disability**
- **lawful sexual activity/sexual orientation**
- **marital, parental or carer status**
- **physical features**
- **political beliefs or activity**
- **pregnancy and maternity**
- **personal association with a person who has one of these personal characteristics**
- **gender**
- **irrelevant criminal conviction**

Explanation
The basic human rights of system users must be protected. Using systems to harass, discriminate against or victimise another system user will be considered misconduct and may result in actions up to and including dismissal being taken under the Council's Conduct and Discipline Procedures.

4.2 The computer systems and networks owned or managed by Buckinghamshire Council are to be used in an effective, safe, ethical and lawful manner. Misuse of ICT resources will be handled in accordance with Buckinghamshire Council's Conduct and Disciplinary Procedures.

Explanation
The computer systems and networks of the Council are primarily for business use and must not be used for illegal or unethical purposes in any circumstances. Illegal or damaging actions or activities whether performed knowingly or unknowingly may be considered misconduct and may result in actions up to and including dismissal being taken under the Council's Conduct and Discipline Procedures.

4.3 The computer systems are to be used for business purposes in the course of normal day to day operations. Personal use must be reasonable and appropriate and not impact on staff productivity, system performance or bring Buckinghamshire Council into disrepute.

Explanation
System performance must not be affected by non-business related activities which may also impact on staff time. All systems, including intranet, internet and email systems are to be used strictly as directed. Where personal use is allowed this is expected to be reasonable and not create additional costs for Buckinghamshire Council.

4.4 Except for guest WiFi, users must not connect personally owned computing devices, computer peripherals, USB devices, digital cameras etc to computer systems or networks owned or managed by the Council. If users do bring personal equipment to work, this is at their own risk and the Council is not responsible for the device or anything stored on it.

Explanation
Connecting personal equipment to networks can jeopardise security, transfer viruses, and allow unauthorised access to information. It is also important for the management and control of computer systems and networks that ICT staff know exactly what devices are connected, who is using them and for what. Malware and malicious code can be introduced and information stolen or disclosed so staff must only use devices that have been provided by the Council for work purposes.

4.5 Encrypted USB sticks allocated by Buckinghamshire Council are only for business use. Extra care is required when storing information on these devices due to their size and portability. Users should be aware of the following:-

- **Loss of the keys and the data is a problem due to the small size of these devices**
- **Increased chance introducing a virus as they can be used on multiple devices**
- **USBs should not be plugged into any computer that does not have up to date security patches and anti-virus software**

- **They must be stored and transported in a safe manner to reduce the chances of theft or loss**

Explanation
Although USB sticks are convenient they introduce a new set of vulnerabilities into the computing environment and users must be aware of the extra care that is required during their use.

4.6 Computer equipment supplied by Buckinghamshire Council must not be altered or added to in any way including:-

- **unauthorised upgrades**
- **addition of components**
- **removal of components**
- **altering configuration or security settings**
- **installation of non-approved applications**

All changes to configuration or maintenance of the device must be carried out by ICT staff or their designated agent.

Explanation
Users must not alter equipment provided by the Council as errors could cause the device to malfunction and void manufacturers' warranties. A user may inadvertently or deliberately bypass security measures, cause confidential or sensitive information to be lost or disclosed and provide an opportunity for hackers to compromise the machine.

In addition, the requirement protects against the removal of internal components like memory chips and helps to ensure the equipment issued to a user is the same equipment that will be returned when the user no longer requires it. This is important where equipment is leased.

4.7 Users must not lend computers, portable devices, tablets, mobile phones, laptops or any other equipment that has been allocated to them by the Council for business activities to anyone external to the Council including friends and family.

Explanation
Staff must not lend the equipment that has been allocated to them to others to use. A wide variety of controls, such as fixed password based boot controls, encryption measures and access controls are set up for a specific individual, given that individual's job duties and the "need to know" principle.

Allowing another person to access that device (except for maintenance which is unavoidable), would allow the other person to access the Council's information. This requirement also gives users a definitive reason for not lending out equipment that has been allocated to them by saying it is against corporate regulations.

This requirement also includes family members who may use the equipment to gain access to the internet or email at home.

4.8 Any actions or activities, whether intended or accidental which cause, or could cause the computer systems, information, or networks of the Council to be compromised in any way is may be considered misconduct including but not limited to:-

- **Security breaches or disruptions of network communications. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.**
- **Port scanning or security scanning. These activities are expressly prohibited unless sanctioned by the Service Director IT for the purposes of testing network security.**
- **Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal duties or has been duly authorised.**
- **Circumventing user authentication or security of any host, network or account or running password cracking programs.**
- **Interfering with, or denying service to any user other than the employee's host (for example, denial of service attack).**
- **Using any program/script/command, or sending messages of any kind, with the intent of interfering with or disabling a user's session using any means either locally or externally.**
- **Downloading, installing or executing any file containing malware which may damage or compromise computer systems or data.**
- **Copying or altering configuration or system files for unauthorised personal use or to provide to other people or users for unauthorised use.**
- **Creating or using open mail relays maliciously, spoofing mail headers, initiating a mail bomb attack or otherwise interfering with the Council's or another organisation's email service.**
- **Downloading or introducing tools or utilities that may potentially be used for hacking activities and undertaking any such activity on any system whether owned or managed by the Council or not.**
- **Providing or selling Council information without approval and for personal gain**
- **Defacing websites, downloading and distributing pornography, running a gambling operation or undertaking any other activity using Council resources that would bring the Council into disrepute.**

Explanation
Users of Buckinghamshire Council's computer systems or networks are prohibited from damaging, disrupting or interfering with the operations of computer systems and networks belonging to the Council or to any other legal entity. Any of the above will be considered misconduct and may result in actions up to and including dismissal being taken under the Council's Conduct and Disciplinary Procedures.

4.9 **Users must use the standard applications for which Buckinghamshire Council is licensed. Do not install any software program, application, script or executable code on equipment in your care. Only software approved by the Service Director IT may be installed on computer equipment owned by Buckinghamshire Council and all installations must be carried out by ICT staff.**

Explanation
In order to maintain a standard ICT environment, strict controls have been created around the installation of code on computer equipment. In some cases software can hog system resources affecting the performance of the machine and installing an application can cause system instability. For example - install a second anti-virus program and it may prevent either of them from working. Automated installation routines are not permitted unless they have the approval of the IT Operations Manager and have been initiated by the Service Desk.

4.10 **Users working in the Council's premises are not permitted to connect to the internet using mobile broadband cards, pairing hotspots, external modems, wireless usb, or any other mechanisms that bypass official corporate systems.**

Devices provided by Buckinghamshire Council have been configured to connect to network resources (including the internet) using approved wired or wireless mechanisms. Use of mobile computing facilities (e.g. mobile broadband cards, wireless usbs or pairing hotspots) may be used when working remotely.

Explanation
To protect computer systems, networks and equipment, all external communications must be routed through corporate channels and the official Internet proxy server. If the user needs a remote connection from a portable device, they should contact the Service Desk who will make the appropriate arrangements.

4.11 **If printing confidential or potentially sensitive information the following must be observed:-**

- **The person authorised to view the information must be present at the printer during printing to ensure no one else reads the document; or**
- **The printer is located in a secure area; or**
- **The document is printed to a storage area on the printer and a code entered or card swiped to initiate the print when the authorised person is present**

The same applies to Scanners, Fax machines and Photocopiers.

Explanation
Unauthorised staff should not have the opportunity to read or copy sensitive printed documents or information that has been received or sent by facsimile. This may be an issue where equipment is shared among work groups or when it is physically located some distance away from the person who initiated the print job.

Where printers, photocopiers, scanners and fax machines are networked it is easy to accidentally send a document to the wrong device or to a device in a public area and users must take care that this does not happen.

Email

5.1 **The email system is predominantly for business use. Personal use must be reasonable and appropriate and not impact on staff productivity, system performance or bring Buckinghamshire Council into disrepute. Misuse will be handled in accordance with Buckinghamshire Council's Conduct and Disciplinary Procedures.**

Explanation
The email system is there to facilitate Council business. Personal use must not affect user productivity or compromise system performance in any way. It is not to be used to conduct outside business or personal activities. If a Manager suspects abuse or excessive use of the email system, a review will be carried out of all communications sent and received by the user.

5.2 **The email system must not be used for any unlawful activity and must not be used to compromise the security or operation of any computer system or network whether it is owned or managed by Buckinghamshire Council or not.**

Explanation
If any user believes that the email system is being used for spamming other email users, in a denial of service attack, to spread viruses or to perform any other illegal action, they must report the incident to the Service Desk immediately. In legislation "not knowing" is not considered a valid defence in the event your computer is used to attack and/or cause harm to others.

It is irrelevant whether the action was intentional or unintentional and either individually and/or in conjunction with Buckinghamshire Council the user could be implicated in any legal proceedings. Misuse will be handled in accordance with Buckinghamshire Council's Conduct and Disciplinary Procedures.

5.3 **Users must not create, send or forward any email messages which contravene human rights legislation and which may be considered discriminatory, victimisation, defamatory, intend harassment or hatred on the basis of:-**

- **Race**
- **Religious Belief or Activity**
- **Sex**
- **Age**
- **Disability**
- **Industrial Association**
- **Lawful Sexual Activity/Sexual Orientation**
- **Marital, Parental or Carer Status**
- **Physical Features**
- **Political Beliefs or Activity**
- **Pregnancy**
- **Personal Association with a person who has one of these personal characteristics**
- **Gender**
- **Irrelevant criminal conviction**

Any of the above actions may be handled in accordance with Buckinghamshire Council's Conduct and Disciplinary Procedures.

Explanation
This requirement is necessary for avoiding legal liability for discrimination, sexual harassment, defamation of character, libel and other employment problems. This requirement is necessary to protect the Council and its employees. Accessing and/or downloading these type of information may be considered misconduct and may result in actions up to and including dismissal being taken under the Council's Conduct and Discipline Procedures.

5.4 **The email system is regarded as an official means of communication and, as such, messages must conform to the same corporate rules for grammar and content as other business communications.**

It is not appropriate to use abbreviations (as used in text messages) or profanities, obscenities, derogatory or sexually explicit remarks in business email messages. Such remarks, even when made as a joke, may upset some people. Special caution is warranted because backup and archival copies of email may be more permanent and more readily accessed than traditional paper communications.

Explanation
Many users consider email to be more informal than traditional paper letters and this can lead to the inclusion of word abbreviations and obscenities or derogatory comments that would not have been included in formal correspondence. Users should treat email correspondence as if it was being written on business letterhead. The requirement also indirectly discourages "flaming" which is the practice of publishing negative emotions via email.

5.5 Users must regularly move corporate emails from email folders to the appropriate records solution. Corporate email is defined as:-

- **E-mail that forms part of the corporate record. It is e-mail that documents the business activities of the Council, e.g. a direction for an important course of action, business correspondence received from outside the Council or a communication between staff members in which a formal approval is recorded.**

Ephemeral emails can be destroyed as part of normal administrative practice. Ephemeral email is defined as:-

- **E-mail used to facilitate the Council's business but which does not need to be retained for business purposes, e.g., notice of meetings, staff movements, copies of reports or newsletters, advertising material and any other publicly available material.**

Personal email should be destroyed as soon as it is no longer required. Personal email is defined as:-

- **E-mail of a personal nature that has no relevance to the business of the Council.**

Explanation
This requirement addresses the usual practice of keeping email in .pst files in personal folders on the C drives of PCs. Important information should be saved as a corporate record and email systems are not designed as archival databases and don't have adequate mechanisms to protect important information.

Email messages stored locally may be deleted by Head of Applications when a user leaves the Council, mistakenly erased by users and lost if hard disk problems occur.

If email has been used in contract negotiations, in the lead up to purchasing or sales, when dealing with customers etc then it must be saved in the appropriate corporate folder. All non-corporate email should be deleted when no longer required.

5.6 Files received from an unknown, suspicious or untrustworthy source must be deleted immediately without opening. Under no circumstances should users click on links contained within an email message sent from an unknown source.

Explanation
If a user suspects there may be something odd about an email message and they don't know the sender, it is important that the file is never opened as this can activate the threat (install malware etc) and cause the computer systems and network to become infected.

Although anti-virus programs protect computer systems up to a point, zero day attacks can still infect systems because vendors take time to update and distribute new virus signature lists.

Information Management

6.1 Data and information created modified saved, transmitted or archived using the corporate systems of Buckinghamshire Council remains the property of the Council.

Explanation
Any document, data or information in any format, irrespective of how it came to be in a system owned or managed by the Council remains the property of the Council including any personal documents and emails.

6.2 All corporate information and data must be stored in approved corporate information repositories.

Explanation
Data needs to be protected from deletion, corruption and loss as required by the Business Continuity/DR Policy.

6.3 All information must be protected based on its sensitivity, value and criticality regardless of the type of media that holds the information, its location, the systems used to process it or the processes it is subjected to. Staff will be trained to recognise unclassified information, especially when it personally identifies individuals.

Explanation
Information must be handled consistently in all cases and data classification rules applied reliably so that electronic information is protected. Where information is particularly sensitive it may require total isolation from other systems and information displayed onscreen or left on desks should not be able to be read from outside the room.

Special consideration may be given to handling media and to managing information throughout its life cycle. When transporting information, or using it offsite the same security requirements must be considered.

6.4 The user must notify their Manager and complete the Online Data Breach Form immediately if confidential or sensitive information is lost, disclosed to unauthorised parties, or is suspected of being lost or disclosed.

Explanation
Prompt notification of confidential or sensitive information loss or disclosure is necessary for performing effective damage control. There is a statutory obligation to report data breaches in certain circumstances within 72 hours.

The SIRO and Service Director IT may be informed in case the disclosure happened as a result of a security breach or system malfunction. In some situations, if the disclosure was found to be malicious then system access may need to be revoked to prevent further activity.

6.5 **Users must not delete or dispose of potentially important Council records or information without the approval of the information owner and without following standard document management procedures for disposing of information.**

Deleting the Council's records without following the proper procedures is considered a serious breach of this requirement particularly if the records cannot be recovered. Such actions may be considered misconduct and managed in accordance with Buckinghamshire Council's Conduct and Disciplinary Procedures.

It should be noted that document retention should be in accordance with the Lord Chancellors Code of Practice on the Management of Records.

Explanation
Once a document has been saved into a document management system it is subject to version control and other records management functions. Use of the record is managed until the end of its useful life as described on the document retention schedule.

Information which is no longer required or is end of life is recorded on a disposal schedule which is signed off by Department Managers and subsequently permanently deleted. Staff must not remove or permanently destroy potentially important information unless records management is their job and the formal process has been followed.

Disaffected staff seeking revenge or to conceal evidence of their actions may go on a file deleting binge, but in most cases files can be recovered from hard drives or backups.

Internet Use

7.1 **The internet is primarily available for business use. Personal use must be reasonable and appropriate, not impact on staff productivity or system performance or bring Buckinghamshire Council into disrepute. A web content control system monitors and controls website visits.**

Explanation
A web content control system must be implemented to monitor use and block inappropriate sites. Line Managers must determine what constitutes acceptable personal use and must maintain a watch on staff browsing habits. The total amount of personal use must not cause the Council to exceed its service plan which will incur additional costs.

7.2 **Buckinghamshire Council monitors and logs web sites visited, files downloaded and social networking accounts controlled by the Council. Line Managers can request reports that allow them to monitor and moderate internet use. Users viewing or downloading content that is deemed inappropriate for the workplace may be subject to disciplinary actions up to and including dismissal.**

Explanation
User internet activities are continuously monitored and logged and Managers can request access to reports that provide information on an individual user's browsing habits. From this information, the Manager is able to gauge whether personal use is appropriate and whether too much unproductive time is spent browsing.

This requirement encourages users to consistently adhere to the Council's Policies and take particular note of their personal use.

7.3 **Users of the internet are not permitted to visit, interact with, or download content from websites that are offensive, obscene or contain indecent material such as pornography or violence. Users must not access, publish or download material which promotes indecent material, hatred or discrimination on the basis of, but not limited to:-**

- **race**
- **religious belief or activity**
- **sex**
- **age**
- **disability**
- **industrial association**
- **harassment**
- **victimisation**
- **lawful sexual activity/sexual orientation**
- **marital, parental or Carer status**
- **physical features**
- **political beliefs or activity**
- **pregnancy**
- **personal association with a person who has one of these personal characteristics**
- **gender**
- **irrelevant criminal conviction**

The above activities should be reported to your Line Manager or Human Resources. All reports will be investigated and handled in accordance with Buckinghamshire Council's Conduct and Disciplinary Procedures.

Explanation
This requirement is necessary to protect the Council and its employees. Accessing and/or downloading these type of information may be considered misconduct and may result in actions up to and including dismissal being taken under the Council’s Conduct and Discipline Procedures.

7.4 **The internet connection must not be used for any illegal or unethical activity or personal business activity and must not be used to compromise the security of any computer system or network whether owned or managed by Buckinghamshire Council or not.**

Misuse must be reported to a Line Manager or Human Resources immediately. Reports of misuse will be investigated and handled in accordance with Buckinghamshire Council's Conduct and Disciplinary Procedures. Examples of unacceptable internet use include but not limited to:-

- **computer hacking (accessing another's electronic data or computer without permission)**
- **providing access to unauthorised persons (including minors)**
- **impersonation**
- **file downloads (except for work related reasons)**

- **use of the internet for personal gain**
- **gaming, wagering or betting**
- **playing games**
- **the intentional transmission in any way of viruses or files that cause a negative impact on computer systems (e.g. unauthorised email attachments such as video, audio and executable files)**
- **downloading or distributing information subject to copyright requirements (such as licensed software or protected internet applications)**
- **disclosing private or confidential information including passwords or other information that may compromise the security of the computer systems**
- **engaging in any illegal activity, including dissemination of material in breach of legislation**

Explanation
Should any user believe that the internet connection is being used for any illegal or unethical activity, they must report the incident to their Line Manager or Human Resources immediately. In legislation "not knowing" is not considered a valid defence in the event your computer is used to attack and/or cause harm to others.

It is irrelevant whether the action was intentional or unintentional and either individually and/or in conjunction with the Buckinghamshire Council the user could be implicated in any legal proceedings.

7.5 Peer to peer file sharing is not permitted. This requirement includes sharing or downloading of movies, music, ebooks, applications, games etc using torrent sharing, torrent clients and file sharing connections.

Explanation
There are at least three issues of concern with the use of file sharing programs as follows:-

- These programs are often used, in breach of copyright, to exchange media files
- Malware can be introduced into the organisation via file sharing. These programs bypass corporate internet virus scanning and shared files are often already infected. Worse, there have been several viruses that specifically target and spread using file sharing programs.
- It is easy to inadvertently share too much information or confidential information.

7.6 When working on their desktop within the Council's premises, users must use the internet connection provided from this equipment. Users must not circumvent internet security by using usb modems, personal hotspots, usb mobile wireless devices and mobile broadband cards. These alternative methods of connecting to the internet will be allocated to users working remotely and the Service Director IT will record all instances where alternative methods of connecting to the internet have been provided.

Explanation
Users may not set up their own internet connection which circumvents the proxy server and corporate security and may not establish their own websites or FTP sites using the Council's systems or equipment.

Users must use the internet connection provided to them and any alternative method of connecting to the internet must be provided by the Council for business use only. The Council reserves the right to inspect equipment at any time to determine whether use of the internet has been appropriate.

7.7 The internet shall not be accessed from another employee's PC, unless the user is logged on with their own user name and password. Administrative and privileged access accounts must not be used when accessing any website or email system.

Explanation
Users are responsible for activities conducted using their user name and password. Sharing passwords or user accounts is not permitted. User activity on the internet is tracked by individual user and should the account show that inappropriate content has been downloaded or malware introduced, then you will be held responsible.

7.8 Personal use of social media sites is permitted using Council equipment during normal work hours. Social media use must be reasonable and appropriate and not impact on staff productivity, system performance or bring Buckinghamshire Council into disrepute. This includes but not limited to:-

- **Social media and news sites, for example, Facebook and Twitter**
- **Video and photo sharing sites such as YouTube and Instagram**
- **Collaborative information sites like Wikipedia**

Access to manage or publish to social media on behalf of the Council is only permitted with the approval of the Communications Team. Participation in work related social media groups, chat groups, list servers or collaborative sites must be conducted in accordance with the Policies and any applicable guidelines.

Explanation
Membership of, or contribution to social networking groups representing the Council is only approved to carry out the day to day business of the Council. Use of social media is not a right for all employees and may only be used in approved situations. If personal use or misuse is identified, those rights will be rescinded.

Social networking websites such as Twitter, Facebook and YouTube are widely accessed by a criminal element that trawls the web looking for personal details to use in targeted phishing attacks. One in every 600 user profiles is infected by malware and statistics show that use of this type of personal blog and video blogs during work time is growing exponentially.

Uploading and downloading videos from YouTube uses the Council's bandwidth and may breach copyright which could implicate the Council in legal proceedings.

7.9 Users must not use social media to cause annoyance or anxiety, to harass, to defame or to transmit unsolicited commercial or advertising material. These actions must be reported to a Line Manager or Human Resources and will be handled in accordance with Buckinghamshire Council's Conduct and Disciplinary Procedures.

Explanation
This requirement advises users of the repercussions of misusing the Council's social media sites. All matters involving abuse or excessive use will be treated seriously.

A certain standard of professionalism is required if users are posting entries to discussion groups or chat rooms and that a certain behavioural code "netiquette" must be followed in all online communications because during work hours users are representatives of the Council and not individuals.

The use of social media on behalf of the Council must have been approved by a Line Manager and social media pages set up to protect the organisation from random postings that may breach this Policy. Pages set up by the Council must be continually moderated to ensure any inappropriate posts are removed immediately.

7.10 Employees are not permitted to create or maintain a blog, wiki or social networking site on behalf of the Council without the express permission of the Chief Executive Officer. Any blog, wiki or shared workspace must have a moderator and an approved code of conduct.

Explanation
These activities must be business focussed and as they may be public facing systems the approval of the Chief Executive Officer is required. The appointment of a moderator will ensure that conduct is appropriate, business related and does not bring the Council into disrepute. A code of conduct sets out the rules for participating in shared online activities so that there are no misunderstandings.

Laptop And Tablet Security

8.1 Corporate information must be transferred to the Council's corporate systems and saved in EDRMS systems or in the appropriate directory on a regular basis. Laptop users should make backups of information stored on the device in between transfers. Information should be copied to portable storage media (CD or USB) and stored in a separate place from the laptop device.

Explanation
This requirement supports other information management requirements with regard to backing up corporate information. If the device is lost or stolen the information is less likely to be lost. Data stored in corporate information repositories is backed up regularly as a matter of course.

Only when there is a necessity to work remotely should confidential data be copied to a local drive on the device and this should be minimised to only that information needed at that particular time. The information should be deleted from the portable device as soon as practicable.

8.2 Users must avoid situations where theft of the laptop or tablet is possible and take the following precautions:-

- **Do not leave the device in view in an unattended motor vehicle**
- **Portable devices must not be left in a vehicle overnight**
- **The portable device should not be visible from any ground floor window unless there is no alternative**
- **Never leave the device unattended for an extended period of time**
- **Secure the portable device with a cable lock or lock it away inside a locked cabinet or drawer when you are not using it**

Explanation
The risk of losing a portable device is greater than normal computers because they are often taken offsite and used in public areas. Laptop computers are often targeted by thieves because they are attractive items and can be easily traded for other items or sold for cash.

Legal Compliance

9.1 **Information and information entrusted to Buckinghamshire Council from third parties falls within one of three main sensitivity classifications. If not designated, the default classification is Internal Use Only. Information that has been classified as personally identifiable (PII) is Official-Sensitive.**

- **TOP SECRET: Information marked as Top secret is that which whose release is liable to cause considerable loss of life, international diplomatic incidents, or severely impact ongoing intelligence operations. Disclosure of such informations is assumed to be above the threshold for Official Secrets Act prosecution.**
- **SECRET: Information which needs protection against serious threats, and which could cause serious harm if compromised - such as threats to life, compromising major crime investigations, or harming international relations.**
- **OFFICIAL: All routine public sector business, operations and services is treated as "OFFICIAL". A limited subset of OFFICIAL information that would have more damaging consequences (for individuals, and organisations or government generally) if it were lost, stolen or published in the media is classified "OFFICIAL/SENSITIVE".**

Explanation
This is the government requirements for information classification issues within the Government Security Classification Policy which took effect in 2014 replacing the old Government Protection Marking Scheme. Its main aim is to protect information based on its classification and it combines the philosophies of “need to know” and “need to withhold” on which all access controls are based.

9.2 **All intellectual property (including patents, copyrights, trade marks, inventions, designs or other intellectual property) created and/or developed by the Council's employees while at work or while using the Council's equipment is the exclusive property of the Council and must be recorded in an asset register.**

Explanation
This requirement supports intellectual property law. Similar clauses are normally included in contractor and consultant contracts where development is being undertaken by third parties.

9.3 **Third party software in the possession of Buckinghamshire Council must not be copied or installed multiple times unless this is allowed by the licence agreement. In all other cases the number of installations should be equal to the number of licences held. Systems will be monitored to ensure software licence conditions are being complied with and licence numbers are not being exceeded.**

Explanation
This requirement relates to software used on personal computers, workstations, servers and other systems and includes application software and operating software.

The intention is to advise users that copying or installation of software must be in accordance with licence agreements so users should not just install one application multiple times unless this is allowed by the licence agreement.

Some software is purchased as multi-user and others may be licenced per instance installed. In some cases escrow arrangements will negate the need for master copies kept for the purposes of system recovery.

9.4 Information held in all computer systems and networks owned or managed by Buckinghamshire Council is subject to the provisions of Privacy legislation and users should be aware of their obligations in respect of managing and using the information and providing information to third parties.

Explanation
Staff must be aware of their responsibilities and conduct their activities in accordance with Privacy legislation as the Council will be liable for any breaches of the law. See the links below or contact Information Governance Team.

Online Services

10.1 When using the Council's computer systems, or when conducting the Council's business, staff must not deliberately misrepresent themselves and, where possible, provide full contact details.

Explanation
This requirement includes participating in online discussion groups and work related social media groups, sending email and establishing user accounts online that require details to be stored on another computer. Use of anonymous FTP log-ins, anonymous UUCP log-ins, HTTP (web) browsing, and other access methods where users are anonymous are exempt from this control.

Access controls are predicated on positive user identification and if this has not been established then the user’s activities cannot be managed, misconduct is difficult to identify and logs are less useful.

10.2 Unless approval has been obtained in advance from the Corporate Management Team users are prohibited from establishing online business to business arrangements or signing up to online services provided via the internet.

Where the online system involves payments or receipts, a secure platform for processing transactions must be approved. Examples include electronic purchasing, personnel management systems, on-line database services, drop box, iCloud, skype etc. Requests for a new online business channel or online service should be made to the Service Desk

Explanation
Departments must not set up their own individual business arrangements through the internet.

There are no international standards for online commerce so it is critical that requests for any new online business channel or service be approved by the Corporate Management Team on the recommendation of the Service Director IT who will verify that any risk to ICT security is within the Council's risk appetite.

All online business arrangements should be conducted through a corporate channel which has been specifically configured to minimise the security risks to Council information and in accordance with any specific requirements mandated by internal auditors and the Corporate Finance Manager.

10.3 Users must not publish corporate information (applications, internal documents or files, press releases, price lists etc.) on any public facing computer system (e.g. website, social media site) unless the item has been authorised by the appropriate Manager and Communications and Engagements for public consumption.

Explanation
Publishing to the internet is no different to publishing in a magazine. Staff are not permitted to release information to outsiders using the internet as a channel unless the release of the information has been authorised by the appropriate Manager and Communications and Engagements.

Buckinghamshire Council has a procedure for publishing to its external website and authors must follow this process. The internal version of information may need to be sanitised before being released to the public and this requirement attempts to protect staff from disclosing sensitive or confidential information and from defamation.

10.4 Financial transactions transacted online must comply with legal requirements, be within approved limits of delegated authority for expenditure and meet the requirements of the Council's financial auditors.

Explanation
There is a requirement for online business systems to meet statutory legislative requirements as well as internal audit and financial requirements. Proof of the transaction that cannot be repudiated in a court of law is required for both purchases and sales made on behalf of the Council over the internet.

It is imperative that these systems are set up with the knowledge of the Service Director IT and the Corporate Finance Manager and be facilitated through corporate computer and communication systems that have been specifically configured to ensure the security of online transactions.

Password And Authentication

11.1 User IDs and passwords must not be disclosed to anyone or shared with anyone.

Group or generic User IDs and passwords are prohibited as a rule, but in special circumstances may be approved by the Service Director IT.

Explanation
This requirement applies to user name and password, PINs, tokens used in multi-factor authentication, door swipe cards and any other forms of identity which should not be shared and also includes shared user identification like group or generic accounts.

Sharing exposes the authorised user to the actions of any other user. Shared user IDs minimise the auditing capabilities of systems and the probability of a password related security breach is increased.

11.2 Passwords must not be written down and left in a place where unauthorised persons might discover them.

Explanation
Discovering passwords written down and left in the top drawer, taped to a computer monitor or in some other conspicuous spot is a common way of accessing computer systems and networks. This is one of the biggest security threats because most users don't realise the implications.

Passwords must not be written down and certainly not written together with the user name and kept near the device it specifically relates to. Users should be able to remember their password and should consider it confidential much the same as the PIN number for their own bank account.

11.3 Staff that use a computer at home should use different login credentials for work and home.

Explanation
There is a high probability that the login name and password used at home are shared with family and others. The user login name and password used to access systems owned or managed by the Council must be kept confidential and this requirement is much easier to adhere to if work and non-work computers use different logins. This requirement lessens the risk that someone who knows you will take advantage of the information they know about you at home and use this to gain unauthorised access to business information.

11.4 Users are responsible for all activity performed with their personal user IDs and passwords. Users must not allow others to perform any activity with their user IDs and are not permitted to perform any activity with IDs belonging to other users.

Explanation
This requirement is important as it establishes a link between a user ID, an individual (and in some cases a software process or a computer system) and the access rights granted to that user. Without unique user IDs, audit logs cannot accurately record the activities of users and this could prevent the Council from being able to take disciplinary action or prosecute for computer abuse.

Personnel Management

12.1 **Breaches of ICT Policies and Procedures will be managed by Line Managers in accordance with the Council's Conduct and Discipline Procedures, seeking advice from Human Resources as required. If the action is inadvertent or accidental, is not unlawful and does not affect Buckinghamshire Council's financial position or reputation or that of any other organisation or individual, a first breach may result in a formal warning.**

The employee will be provided with training to ensure that the error does not occur again. Subsequent breaches, including those considered willful or intentional may be considered misconduct and will be subject to internal disciplinary actions that may include termination of employment and/or legal proceedings.

Explanation
Buckinghamshire Council has a Conduct and Discipline Procedures document which is updated from time to time by the Human Resources Policy and Reward Team in accordance with employment law. Line Managers will take responsibility for implementing and overseeing the procedure if it becomes necessary to take disciplinary action against a member of their staff.

12.2 **Staff must avoid actual or potential conflicts of interest in their capacity as an employee and conducting business on behalf of the Council and if there is any doubt about a particular situation they should consult their Line Manager.**

Explanation
There must be no conflict of interest between personal and work related dealings that staff have with the Council. In the area of ICT this situation could eventuate where a staff member evaluating a tender for the purchase of computer equipment has a connection with one of the businesses submitting a tender or where the Head of Infrastructure responsible for system configuration has a relationship with a person conducting a system audit.

Remote Access

13.1 **Remote users are only permitted to access applications and systems they have been approved to access for the purposes of fulfilling obligations to Buckinghamshire Council.**

Explanation
For security and privacy reasons access privileges for users must be limited to the ICT resources and information needed to achieve business objectives. These access privileges must be reviewed every six months to ensure they are still required.

13.2 **Users must not be remotely connected to Buckinghamshire Council while concurrently connected to another network or initiate a connection to another network during the period they are connected to the Council. This practice is called split tunneling.**

Explanation
The practice of connecting to two locations simultaneously is called split tunnelling and must be prevented through the correct configuration of settings in the remote access client.

This requirement is essential to prevent information leakage and potentially the loss of important and/or confidential information as it is a known method used by hackers to extract information to sell on the black market. It also allows a hacker to use your machine as a gateway to attack the network you are connected to so it looks like you did the hacking.

13.3 The Council reserves the right to monitor and audit the use of remote access connections. Logs containing details of user activities may be retained.

Explanation

The Council reserves the right to monitor and audit remote connections using any tools and applications it deems fit to determine that the remote link is being used in accordance with ICT Policies and Procedures and that the appropriate levels of security are maintained.

Employee Acceptance

I have read, understood and agree to abide by the Buckinghamshire Council Acceptable Use Policy.

Signature _____ Date _____

Name of Employee _____

Department _____

Please **return this signed page** to Human Resources and **retain the policy** for your reference.