



Internet, Email and Computer Usage Policy



TABLE OF CONTENTS

TABLE OF CONTENTS	0
Document Control	2
Document History	2
1. Policy Objective.....	3
2. Policy Statement	3
3. Definitions	3
4. Responsibilities	4
5. Recommended Practices	4
Use of facilities	4
Legal issues	4
Authorisation of Use	5
6. System Security	5
Responsibility of the Manager of Business & Governance in consultation with Councils IT employees.....	5
Passwords.....	5
Communications System Security.....	5
Hardware, Software and Privileges	5
Streaming.....	6
7. E-mail Usage.....	6
Privacy	6
Management of E-mail Messages	6
Standards for Outbound E-mail.....	7
Acceptable personal use of e-mail	7
Unacceptable use of e-mail.....	7
What you should do if you receive offensive e-mail.....	8
Limitations	8
8. Internet Usage.....	8
Access to sites	8
Sending information	8
Acceptable personal use of internet facilities.....	8
Unacceptable use of internet facilities	8
Social Media.....	9
9. Personal Use – General	9
Acceptable Personal Use	9
Work Related Study Use	9



Copyright.....	10
10. Other Issues	10
Workplace Health and Safety	10
Education and Training	10
Monitoring and Auditing of Equipment, Services and Software	10
11. Compliance with Policy	10
Read the policy.....	10
Conditions of employment.....	11
Breaches of the policy	11
Variations	11
Internet Disclaimer	11
Commitment.....	11
12. Appendix A - Social Media Account Checklist.....	12
13. Appendix B – Councillor / Employee User Agreement	14



Document Control

Policy	Internet, Email and Computer Use Policy	Policy Number	TBA
Author/Reviewer	Executive Director Corporate & Community	Review Period and Date	Reviewed within 12 months of election/4 yearly - September

This policy shall be reviewed: -

- This document will be reviewed within 12 months of an election, and thereafter at four yearly intervals, or as otherwise determined by Council. This will include the issue of a new Modal Plan by the NSW Ombudsman.
- This policy commences as from the last date of adoption by Council as listed in the document history and replaces all previous versions.

Document History

Date	Status	Version	Resolution	Description
26 October 2017	Draft	0.1		Presented to Consultative Committee for review and endorsement
26 October 2017	Draft	0.2		Endorsed by Consultative Committee for review by the Policy Committee
28 February 2018	Draft	0.3		Presented to Hilltops Council for endorsement, public exhibition 28 days.
28 February 2018	Draft	0.4	18/26	Endorsed for public exhibition – 28 days
28 March 2018	Final	1.0	18/26	No submissions received – policy adopted



1. Policy Objective

The objective of this policy is to provide clear guidelines for the use of computers, internet, e-mail and other electronic media and devices to allow effective use of Council resources and clear communication with Council both internally and externally.

Elected Councillors and employees will be required to sign-off on this policy at the commencement of their term/employment to certify that they understand and agree to comply with the terms of this policy.

Council has given Councillors and employees access to telecommunications, e-mail, computer, internet and other facilities to assist them to communicate effectively with each other and others with whom Council communicates, and to use the information gathering and storage capabilities that the facilities provide. Council also recognises that occasionally, Councillors and employees may wish to use the facilities for private purposes, to meet family and community responsibilities.

2. Policy Statement

The unique nature of internet, e-mail and computer facilities is supported by this policy which has the purpose of;

- Preserving the integrity and efficiency of the facilities by providing guidelines for Councillors and employees to clarify what constitutes appropriate conduct and use of the facilities;
- Outlining the expectations Council has of the manner in which Councillors and employees will use the facilities, so that they enhance the professional and personal lives of Councillors and employees, while complying with the organisation's obligations to maintain a workplace that is efficient, harmonious and without risk of discrimination or harassment resulting from improper use of the facilities; and
- Outlining to Councillors and employees what will happen if they fail to abide by the guidelines contained in this policy.

3. Definitions

Council means Hilltops Council

Computer Equipment means and includes any electronic equipment or computer software, provided to Councillors and employees for use in the performance of their duties, either in general or specific terms, including, but not limited to;

- Computers, including PC's, laptops/notebooks, tablets and handheld devices;
- Printers;
- Scanners;
- Digital cameras or any other digital imaging equipment;
- All software and programs provided to facilitate work needs;
- Network operating systems (eg Windows);
- All network infrastructure including data cabling and transmission equipment;
- All forms of e-mail;
- Internet access
- Mobile phones connected to the internet and/or email

Council's Record Incorporates Policies, Procedures and Protocols in place from time to time



Management Procedures	incorporates Policies, Procedures or Protocols in place from time to time which determine how business records are received, stored, actioned and referred throughout the organisation.
Normal Working Duties	means and includes all activities associated with fulfilling the duties and obligations of the Employee's Position Description.
Privileges	means and includes the specific permission granted to access and/or use Computer Equipment including areas where electronic files may be stored, modified or viewed and the quality of such storage space which will be made available.
Streaming	means Multimedia (audio and video) files that are available to play in a steady and continuous flow, almost immediately upon their downloading.
Work Related Study	means and includes study and research approved by an employee's relevant Director for the purpose of developing skills required in the performance of their position.
Social Media	means a group of Internet-based applications that build on the ideological and technological foundations that allow the creation and exchange of user-generated content. Furthermore, social media depend on mobile and web-based technologies to create highly interactive platforms through which individuals and communities share, co-create, discuss, and modify user-generated content.
Authorised Officer	means and includes the following positions; <ul style="list-style-type: none">• General Manager• Executive Director of Corporate & Community• Director of Infrastructure• Director of Sustainable Growth• Chief Financial Officer• Manager Business & Governance

4. Responsibilities

This policy applies to all Hilltops Council employees, Councillors, work experience students and volunteers.

5. Recommended Practices

Use of facilities

Council has provided the facilities primarily for business purpose and to enhance the productivity and quality of work. Private use of facilities in the case of staff should be restricted to breaks.

Legal issues

Council and its Councillors and employees may be legally liable if the facilities are used in an unlawful way. The following legislation is relevant:

- NSW Anti-Discrimination Act 1977;
- NSW Privacy and Personal Information Protection Act 1998;
- NSW State Records Act 1998;
- Evidence Act 1995;
- Federal Sex Discrimination Act 1984;
- Federal Disability Discrimination Act 1992;



- Federal Racial Discrimination Act 1975;
- Federal Crimes Act 1900;
- Federal Copyright Act 1968;
- Federal Defamation Act 1974;
- Defamation Act 2005 (NSW);
- Employees Liability Act 1991 (NSW); and
- Crimes Act 1914 (Cth).

The guidelines in this policy are based upon the requirements of this legislation, so as to protect both Council and its Councillors and employees from legal action.

Authorisation of Use

Employees and Councillors will be granted privileges to use computer equipment supplied by the Council, following confirmation of their employment/election and the required authorisation forms being completed by an authorised officer.

6. System Security

Responsibility of the Manager of Business & Governance in consultation with Councils IT employees

It is the responsibility of the Manager of Business & Governance in consultation with Council's IT employees to provide, maintain and monitor the necessary hardware and software (eg Anti-Virus) to minimise security risks.

Passwords

It is the responsibility of each employee and Councillor to maintain the confidentiality and security of their own password. Councillors and employees should ensure that they;

- Log off the network or password lock their workstation whenever leaving it unattended for long periods of time, including attending meetings and lunch breaks;
- Do not attempt to gain access to another employee's or Councillor's log-in id or password; and
- Do not disclose passwords to any other persons.

Persons who are not employed by Council (including Councillors) must not be given access to the Council's corporate network under any circumstances, unless approval is first sought and obtained from the General Manager. This includes work experience students, volunteers, etc. Where approval to access equipment and software is conditionally given, such persons are not permitted to use an existing user's log-in id or password. In such circumstances, an authorised officer will arrange a temporary account with the appropriate security privileges.

Communications System Security

To help avoid the spread of viruses, Councillors and employees must not by-pass Council's network security by accessing the internet directly by modem or other unauthorised means, unless permission has been granted by an authorised officer.

Councillors and employees using IT equipment with access to Council's network and not utilising Council supplied IT equipment, must ensure that any file or data brought into Council from an external (to Council) source, is scanned with Council approved virus checking software. The Executive Director of Corporate & Community must be notified immediately, if any employee or Councillor suspects that a virus has been introduced into Council.

Hardware, Software and Privileges

Councillors and employees must not attempt to install or remove software or hardware onto Council's Computer Network without prior approval and direction from an authorised officer.



Streaming

Streaming material via Council's network utilises bandwidth and slows network performance. Therefore, no network users are permitted to "stream" without authorised consent.

As a requirement of the State Records Act, all Council information and/or data is to be permanently stored on Council's servers for backup and security implications. Therefore, disk space on individual Council PC's or Council laptops, should only be used as temporary storage, or for transitional purposes only. Please note that in general, Council PC's or Council laptops are not backed up in any way.

Councillors and employees must not attempt to access, copy, damage, delete, insert or alter any information held on Council's Computer Equipment beyond the Privileges granted by an Authorised Officer for the performance of their normal working duties.

7. E-mail Usage

Privacy

E-mail is made available to Councillors and employees primarily to enable Council to conduct its business communications efficiently. All e-mails sent or received from Council's system remain the property of Council. For legal purposes, email has the same standing in court as paper documents.

Councillors and employees should not expect that e-mail is confidential or private. Therefore, when sending confidential information (for example business information, client details, pricing, or any personal or private information about individuals), careful consideration should be given as to whether alternative means of communication are preferable.

Whilst Council does not wish to become a censor, to ensure that the guidelines contained in this policy are followed, council retains the right to access or view users' e-mail sent via the corporate network. Council will only access information created or stored on Council's e-mail system for disciplinary procedures or where there is a valid business requirement.

Management of E-mail Messages

E-mail is a valid form of communication within Council. Councillors and employees should attempt to access their e-mail at least once per day. Councillors and employees must manage their e-mail mailbox personally by ensuring that e-mails received are actioned within acceptable times, unwanted e-mails are cleared, and business communications are registered in accordance with the State Records Act of 1998, e-mail messages are official records of Council's business and the legislation requires Council to be accountable for that business. Transactions that provide evidence of business activities, which include but are not necessarily limited to;

- What happened;
- What was decided;
- What advice was given;
- Who was involved;
- When it happened; and
- Order of events and decisions.

are required to be documented in the Records Management System to provide an official record.

E-mail messages that document such activities, should be forwarded electronically to mail@hilltops.nsw.gov.au for registration into the Council Records Management System.

When Councillors and employees go on leave, it will be their responsibility to ensure that arrangements have been put in place while they are on leave, so that their emails can still be processed or acknowledged in some way.



Standards for Outbound E-mail

The content of e-mail signature files is to clearly state the identity of the e-mail originator. Councillors and employees should include their name, title, telephone number, email address and Council website address with a high-resolution image of Council's logo on all e-mails.

Example;

<NAME>

<POSITION TITLE>



Locked Bag 5 **Mobile** XXXXXXXXXX

YOUNG NSW 2594 **Phone** (02) 6380 1200

<name>@hilltops.nsw.gov.au **Fax** (02) 6385 3562

Boorowa Office – 6-8 Market St Harden Office – 3 East St Young Office – 189 Boorowa St
BOOROWA HARDEN YOUNG

DISCLAIMER: The information contained in this email message and any accompanying files is, or may be, confidential. If you are not the intended recipient, any use, dissemination, reliance, forwarding, printing or copying of this email or any attached files is unauthorised. This email is subject to copyright. No part of it should be reproduced, adapted or communicated without the written consent of the copyright owner. If you have received this email in error, please advise the sender immediately by return email, or telephone and delete all copies. Hilltops Council does not guarantee the accuracy or completeness of any information contained in this email or attached files. Unless otherwise stated, the opinions expressed in this email are those of the writer and do not necessarily represent those of Hilltops Council. Information contained in this email should not be relied upon where loss, damage or injury is possible. Internet communications are not secure and Hilltops Council does not accept legal responsibility for the contents of this message or attached files.

[Please consider the environment before printing this e-mail](#)

Acceptable personal use of e-mail

Council accepts that e-mail may on occasion be used for personal reasons. Acceptable personal use includes sending short personal e-mails preferably during lunch breaks or outside normal work hours. However, Councillors and employees must remember that the primary purpose of the e-mail system is to enhance business communication and hence, the overall effectiveness of the organisation. Excessive personal use of the e-mail can undermine that effectiveness and lead to disciplinary action.

Unacceptable use of e-mail

Councillors and employees must not access, or attempt to access, another employee's or Councillor's e-mail while in transmission or stored on a system without authorisation from the employee or Councillor whose e-mail is to be accessed, or an authorised officer. Any e-mails caught by virus cleaning software will no longer be considered private and will be open for interrogation by the General Manager, Directors or an Authorised Officer.

Councillors and employees specifically must not use e-mail (including personal e-mail) to;

- Conduct illegal activities;
- Send e-mail messages that in any way could, or would be likely to bring Council's name into disrepute;
- Send e-mail messages (with or without attachments) which contain inappropriate or offensive material of a sexual, racial, libellous, defamatory, abusive, obscene or discriminatory nature;



- Distribute “junk mail” or electronic chain letters including letters seeking donations and those providing pyramid selling schemes or advertising;
- Send unauthorised e-mails from another person’s e-mail address or impersonating another person;
- Send e-mails which are likely to be perceived as harassment, intimidation or an unwanted invasion of privacy;
- Send non-urgent e-mails (e.g. jokes) to large numbers of people (whether within Council or not) at any time; and
- Send personal e-mail to any person who does not wish to receive it. If a recipient asks a user to stop sending him or her e-mail, their request must be observed.

What you should do if you receive offensive e-mail

If an employee or Councillor receives offensive e-mail from outside Council, they should immediately delete it. In the event that further material is received, the employee should advise their supervisor. A councillor should advise the General Manager.

Limitations

Council has implemented a maximum size for allowable e-mail messages and also restricts e-mail messages that contain certain attachments or content which have been known to contain viruses from either entering or leaving Council. Users will be notified by (return) e-mail, when such limits have been exceeded. An authorised officer should be contacted on a case by case basis, if these limitations are found to be too restrictive.

8. Internet Usage

Access to sites

Councillors and employees should be aware that internet sites accessed by them can record Council’s name. Council can monitor sites that Councillors and employees are accessing and it reserves the right to do so, to ensure that the guidelines contained in this policy are followed. Council reserves the right to block access to sites which it deems to be inappropriate.

Sending information

The internet is not a secure method of sending information. Therefore, when sending confidential information (for example business information, client details, pricing, or any personal or private information about individuals), careful consideration should be given as to whether alternative means of communication are preferable.

Acceptable personal use of internet facilities

Council accepts that the internet facilities may on occasion be used for personal use reasons. Acceptable personal use includes browsing the internet during lunch breaks or outside normal work hours. However, Councillors and employees must remember that the primary purpose of the internet facilities is to enhance business activities and hence, the overall effectiveness of the organisation. Excessive personal use of the internet facilities can undermine that effectiveness.

Unacceptable use of internet facilities

Councillors and employees specifically must not use the internet facilities to;

- Intentionally access sites which contain pornography, or inappropriate or offensive material of a sexual, racial or discriminatory nature;
- Solicit, download, store, or distribute pornography, inappropriate or offensive material of sexual, racial or discriminatory nature;
- Access internet chat clients or internet relay chat networks;
- Conduct gambling activities;
- Conduct private transactions of a personal gain/profit nature, either directly or indirectly;
- Conduct gaming activities during working hours; and
- Stream music or programs as these activities utilise significant bandwidth and has a detrimental effect on Council’s activities.



Social Media

Hilltops Council recognises that social media provides new opportunities for dynamic and interactive two-way communication which can complement existing communication and further improve information, access and delivery of key services.

When establishing a social media account on behalf of Council, users must complete the Social Media Account Checklist (Appendix A) and submit to the relevant Director for approval and the General Manager for authorisation.

All log in details and passwords must be supplied to records and stored in Council's Record Management System in a confidential folder.

9. Personal Use – General

Acceptable Personal Use

Notwithstanding the concessions made for acceptable personal use of e-mail and internet facilities in above sections, Council accepts that its Computer Equipment may on occasion be used for personal use reasons. Acceptable personal use includes the following, conducted during lunch breaks or outside normal work hours and consistent with all other sections of this policy;

- The creation and storage of personal computer files, up to a total of 100 Megabytes at any one time, and which must be stored only in the section allocated for personal files on Council's Corporate Network; and
- The limited use of printers with the verbal (or written) agreement of an authorised officer.

However, Councillors and employees must remember that the primary purpose of Council's computer equipment is as a tool for business and hence, to enhance the overall effectiveness of the organisation. The provision and maintenance of computer equipment and consumables is a cost to Council's business activities and therefore excessive personal use of these facilities can undermine the effectiveness of the organisation.

Councillors and employees must not use Council's computer equipment to maintain or support a personal business activity under any circumstances.

Work Related Study Use

Use of Council's computer equipment, including e-mail and internet, may be granted to an individual Councillor and employee for work related study purposes by agreement with an authorised officer.

This agreement must;

- Be consistent with all sections of this policy.

The agreement may:

- Be for a fixed period;
- Contain limits on the equipment available for use;
- Contain limits on the time periods when study use may take place;
- Require that records of use are to be maintained;
- Detail the apportionment of costs associated with the usage; and
- Permit variation by mutual agreement at any time.

Agreements for Work Related Study Use may be revoked at any time by an authorised officer by written or verbal notification to the employee or Councillor.



Copyright

All Councillors and employees must respect the copyright and any other intellectual property rights of third parties.

Copyright protects the exclusive right of the copyright holder to copy, publish, perform, broadcast and sell copyrighted material. Councillors and employees must not download material from the internet or otherwise receive and use information that is owned by a third party unless they have the written permission of that party.

Examples of possible breaches of copyright can include forwarding e-mails or copying or downloading copyright material (including computer programs, screensavers, sounds and images) that have copyright protection.

As a general rule, under copyright law downloading from the internet for personal research is allowed. However, downloading material for distribution to others or for business purposes will require the permission of the third-party owner.

10. Other Issues

Workplace Health and Safety

It is the responsibility of Council to ensure;

- Councillors and employees are aware of any relevant issues pertaining to the correct handling and usage of computer hardware and software; and
- That monitors meet current Australian safety standards.

Councillors and employees must ensure:

- That all cabling is arranged tidily so as not to present a health or operational hazard; and
- That equipment is used in accordance with guidelines of this and other Policies and Procedures as may be adopted from time to time.

Education and Training

It is the responsibility of supervisors in the case of staff and the General Manager in the case of Councillors to ensure Councillors and employees are made aware of the contents and purpose of this policy, and compliance requirements of the policy.

Monitoring and Auditing of Equipment, Services and Software

Councillors and employees must be aware that;

- Computer usage, including internet access and e-mail, will be monitored to ensure that the guidelines contained in this policy are followed. This includes monitoring personal usage of computer equipment during and out of normal work hours;
- Logs may be kept indicating internet sites Councillors and employees have visited; and
- Authorised officers may request such monitoring to take place with respect to an employee for which they are responsible, and may view such monitoring or logs as are available.

11. Compliance with Policy

Read the policy

All Councillors and employees must read this policy carefully and observe its requirements. It is the employee's and Councillor's responsibility to ensure that they understand their obligations in relation to the policy.

Councillors and employees must also sign the attached acknowledgement of understanding form prior to being granted access (or continuing access) to the facilities.



Councillors and employees must not sign unless they fully understand and agree to comply with all the terms of this policy.

Conditions of employment

Compliance with this policy is a condition of each employee's employment with Council. A breach of any part of this policy may, depending on the circumstances, be regarded as a serious breach of any employee's employment contract with Council.

Breaches of the policy

A failure to comply with this policy and any relevant directions given by management may result in the following action being taken against an employee or Councillor;

- Counselling (including intensive training on this policy and the appropriate use of facilities); and/or
- Disciplinary action regarding "inappropriate use" of the facilities, including cancellation of access to any or all of the facilities; and/or
- Dismissal in cases of staff such as the access and/or distribution of material outlined in the unacceptable use of e-mail or unacceptable use of internet facilities sections of this policy.
- Code of Conduct proceedings

Variations

The policies and procedures at Hilltops Council are the management tool developed to assist in operational requirements. This policy may be reviewed, varied or revoked according to these requirements. No change will take effect until it has been appropriately communicated to Councillors and employees.

Internet Disclaimer

Upon accessing the internet via the Council's network, you immediately release, discharge and indemnify Council of all liability and responsibility;

- With respect to defamatory or other offensive material that you may access on the internet by reason of web searching and browsing by you;
- Relating to any costs incurred associated with the use of on-line shopping services or any monetary transaction undertaken by the employee or Councillor not directly relating to Council business;
- With respect to the unauthorised use of copyrighted material obtained via the internet.

Commitment

Councillors and employees are required to initially commit to this policy by signing this document to acknowledge that they have read the policy and agree to comply with its terms.

References

- NSW Anti-Discrimination Act 1977;
- NSW Privacy and Personal Information Protection Act 1998;
- NSW State Records Act 1998;
- Evidence Act 1995;
- Federal Sex Discrimination Act 1984;
- Federal Disability Discrimination Act 1992;
- Federal Racial Discrimination Act 1975;
- Federal Crimes Act 1900;
- Federal Copyright Act 1968;
- Federal Defamation Act 1974;
- Defamation Act 2005 (NSW);
- Employees Liability Act 1991 (NSW); and
- Crimes Act 1914 (Cth).
- Hilltops Council Code of Conduct
- Hilltops Council Communications Policy



12. Appendix A - Social Media Account Checklist

The following checklist is a good place to begin when considering setting up a social media account and determining its purpose.

1. What will our account name be?

- Can we get a name that aligns with our organisation-services?
- Can we get a name that matches other social media accounts we already have?
- All Council pages must commence with “Hilltops” followed by the position or department title (eg Hilltops Council Mayor) or a position or department title followed by “Hilltops Council” (eg General Manger Hilltops Council).
- All Council social media pages are owned by Hilltops Council.

2. What email account will it be linked to?

- Can this email be accessed by multiple Councillors and employees or one person only?
- If it is a corporate account will it block communication from the site?

3. Who can post/publish items to the account?

- Will publishing responsibility be restricted to an individual or team of people?
- How will the messages be controlled, fact checked, spell checked?
- Is it important that any communications have a similar ‘voice’ or style?
- Will this be officially recognised as part of people’s work plans with time allocated to the activity? If so, how much time?

4. What type of content can be published?

- What will the account be used for primarily?
- Will we post images or just text?
- Will we post details of events/promotions for organisations outside of Council that we are not a partner with, or attending?
- Will we post details of events/promotions for other areas of Council?
- What about activities/groups that Councillors and employees are involved with outside of work?
- What is our policy about naming Councillors and employees members online?
- What do we do with information that may be critical of Council or politically sensitive e.g. new development application?

5. Who is our target audience?

- How will we reach them?
- Why are we doing this?

6. Who/what will we follow/friend or NOT?

- Will we follow official Council accounts from our own Council?
- Will we follow other Councils?
- Will we follow local media?
- Will we follow Councillors?
- Will we follow individual members of Councillors and employees?
- Will we follow members of the public?
- Will we follow political parties?
- What about legal service providers, businesses, emergency services, Government organisations, community groups, lobby groups, clubs etc.?



7. Who/what will we block and why?

- What is our legal/moral obligation here?
- Will we block illegal, offensive, defamatory material? Political/fundraising material?
- Advertising/promotional material?

8. Will we Direct Message followers/friends?

- Will our communication/posting be public? – remember many of our followers/friends may be under 18 years of age.

9. How will we track/monitor our postings/communication?

- Will we use a third-party product?
- What will our policy be about deleting posts?
- Should copies be kept of deleted posts?
- Do we need to archive posts? How often? How?

13. Appendix B – Councillor / Employee User Agreement

IT USER PROFILE CREATION/AUTHORISATION FORM

(FCR-523)

I _____ have read, understand and agree to comply with the terms of the Email and Internet and Computer Use Policy, which governs the use of Hilltops Council's technology systems.

I understand my responsibilities as a user on the Hilltops Council network.

I further understand that any violation of the Email and Internet User Policy and Procedures is unethical and may constitute a criminal offence. Should I commit any violation, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Councillor/employee Signature: _____ Date: _____

PLEASE MARK ALL RELEVANT BOXES																											
<input type="checkbox"/> Internet Access <input type="checkbox"/> Email Address _____@ <input type="checkbox"/> Microsoft 365 Software profile <input type="checkbox"/> Network profile – access to _____ Department drives <input type="checkbox"/> Mobile Phone – DATA Y / N (_____GB p/mth) <input type="checkbox"/> Others eg. MapInfo, SIX Maps, COMMBIZ _____ _____	<input type="checkbox"/> CIVICVIEW <input type="checkbox"/> CIVICA <input type="checkbox"/> FUJITSU (please mark any that apply M for maintenance or E for enquiry) <table border="1"> <tr><td>Property – Land</td><td></td></tr> <tr><td>Property – Rates</td><td></td></tr> <tr><td>Applications/Registers</td><td></td></tr> <tr><td>Correspondence</td><td></td></tr> <tr><td>Customer Services</td><td></td></tr> <tr><td>Work Orders</td><td></td></tr> <tr><td>Ledgers/Jobs</td><td></td></tr> <tr><td>Creditors/Debtors</td><td></td></tr> <tr><td>Financial Parameters</td><td></td></tr> <tr><td>Orders (purchase delegation \$_____)</td><td></td></tr> <tr><td>Assets</td><td></td></tr> <tr><td>Payroll</td><td></td></tr> <tr><td>Human Resources</td><td></td></tr> </table>	Property – Land		Property – Rates		Applications/Registers		Correspondence		Customer Services		Work Orders		Ledgers/Jobs		Creditors/Debtors		Financial Parameters		Orders (purchase delegation \$_____)		Assets		Payroll		Human Resources	
Property – Land																											
Property – Rates																											
Applications/Registers																											
Correspondence																											
Customer Services																											
Work Orders																											
Ledgers/Jobs																											
Creditors/Debtors																											
Financial Parameters																											
Orders (purchase delegation \$_____)																											
Assets																											
Payroll																											
Human Resources																											

I hereby authorise the abovementioned employee/Councillor to use the nominated computer software/profiles

APPROVED BY DIRECTOR		APPROVED BY GENERAL MANAGER	
_____	/ /	_____	/ /

Completed by: _____ Date: _____

Network User Name: _____	Password: _____
Email prefix: _____	Password: _____