Smart Guide No. 5

Social Media, Mobile Devices, Internet, and Email in the Workplace

Supporting documentation and letter templates may be found in Tool Packs No.1 and 2.

This will be indicated in the text by the following: (TP1) or (TP2).

All information contained in this guide is current at time of release.

Introduction

In today's world the mode and speed of changes in technology and communication have altered traditional habits and behaviours in a manner that will only increase in intensity and methodology. These changes have fundamentally altered the way that people in general communicate in both their private lives and in the workplace.

The difficulty for employers is that the pace of change in many organisations has overtaken their existing policies and procedures and they are struggling to get a handle on what they should do, what they can do and how to do it.

Smart Phones, tablets, faster internet connections, greatly improved computer capacity and capability combined with the exponential growth and use of the internet and artificial intelligence in general have created a new workplace where sales, marketing, corporate information and business transactions are mainly online. The rapid decline of institutions such as telephone directories, printed city maps (replaced by GPS devices and web-based map applications) and other information mediums has been taken to the level where information, when required, can easily be accessed by going online with a multitude of devices from personal computers to the everyday Smart Phone. Google maps provides directions, yellow pages online provide searches for business contacts and white pages online will supply personal contacts. Sites such as eBay will buy or sell just about anything. Google has become an almost universal search engine used to answer questions on any topic imaginable, with YouTube and a multitude of spin offs and clones providing videos ranging from stupid and dangerous pranks to more practical matters. Information on any subject is now available online and often (with the increase in collaboration over the internet) with much more detail and accuracy than ever before.

Like any societal change, the increases in technology have also filtered through to the workplace. On the more extreme end there is a huge amount of pornographic material online (which continues to provide problems in the workplace), and you can also find sites from how to build a bomb to personal information on competitors and work colleagues. A Google survey discovered that approximately $3,000 per second is spent accessing online pornography and this relates only to the paid sites, with 12% of all internet content being pornography and the industry being worth approximately $96 billion in 2019. The compounding problems associated with this issue are when employees access this type of material at work and then retain or forward the material to co-workers which can give rise to sexual harassment, workplace discrimination and bullying claims. This access to information and the amount and volume of material available means that employers must ensure that staff (particularly those with access to computers at work) are gainfully employed and do not waste work time surfing the internet or indulging in inappropriate or unlawful behaviour.

The first point of defence is to ensure your computers are protected by an appropriate security software program which can provide reports on access and use and can be programmed to selectively filter online use and access.

Where this type of software or monitoring is in place all staff need to be advised of:

- The conditions of use of their computer equipment
- What is monitored
- What online access is allowed?
- What online access is prohibited?
- The consequences of breaches of these requirements

The best and most practical way to ensure compliance is to have up to date policies in place which cover your particular workplace circumstances, equipment, online structures, and access requirements.

This Guide will provide some practical views and recommendations on how to deal with online issues, particularly social media, the internet and the use and abuse of email.

Smart Phones, Tablets and Other Mobile Devices

A recent survey conducted by Deloitte's found that approximately 89% of Australians owned a Smart Phone, 60% owned a tablet and 53% owned a Smart Phone, personal computer, and tablet.

The proliferation of these devices combined with the ever-increasing technological capability of these devices creates some complex dilemmas in the workplace for employers.

Many employers supply mobile phones, laptops, or tablets to employees as part of their role or employment conditions.

Where these devices are supplied, it is important to distinguish between business and private use.

The general principles as contained in this Guide in relation to unauthorised, illegal, and private use still apply, and Option 2 in the policy options contained at the end of this section covers the circumstances where Smart Phones etc. are supplied.

Smart Phones

Current Smart Phones are much more powerful now than basic desktop computers were only a few years ago.

Employees can perform a multitude of functions on their Smart Phone apart from making and receiving telephone calls, some of which are listed:

1. Personal emails
2. Personal banking
3. Messaging
4. Online forums
5. Facebook, Instagram, Twitter, Snapchat etc.
6. Research almost anything
7. Obtain information and quotations for almost anything
8. Find tradesmen, builders, or any service personnel
9. Travel arrangements
10. Plan weddings or any other type of social event

The list is literally endless; however, due to the fact that these Smart Phones can be kept in an employee's pocket, drawer, bag or car, the possibility that they can be used to carry out tasks which are not in the employer's interest increases exponentially.

The days of an employee having their phone available for emergency calls has been replaced with an almost obsessive ownership of Smart Phones that are in almost every workplace and regularly checked by their owners for activity and updates.

With the introduction of larger phones with clearer screens, and video streaming services such as Netflix and Stan and others that provide television, movies and games online, it is possible for an employee to watch a movie or other entertainment while sitting at their desk without a computer being supplied.

They can do their banking, check on the kids with online cameras, chat with friends, manage their travel and home maintenance, order their groceries and just about anything else from a small handheld, easily concealed private device.

When an employee is logged on to a workplace desktop computer, it is relatively easy to monitor their online and work activity and manage their output and deliverables.

However, as the employee's Smart Phone is their own private equipment, the employer has no way to monitor the activities taking place, or the time spent on the employee's Smart Phone.

Another area of concern is that these devices can be used in the workplace to access prohibited sites such as pornographic material and gambling sites.

This issue has the ability to dramatically reduce an employee's commitment and time spent on actually performing the tasks that they are employed to perform.

There have been recent cases where employees have been filmed at work inappropriately by a work colleague and as part of the action, the employer has been found partially responsible for the actions by not having suitable policies and procedures in place to prevent this type of behaviour.

Tablets and Laptops

Laptop computers are gradually being replaced with more portable and user-friendly tablets that connect to a keyboard and have similar capabilities to a desktop personal computer.

These devices come in a variety of brands and sizes and are often easily concealed by employees and again, if an employee is spending time on one or more of these devices, their activity cannot be monitored by the employer.

Employee Policies

It is therefore crucial that your employee policies adequately cover the circumstances suitable for your workplace, and the devices that may be used by your employees at your workplace.

Some options which may be included in your policies include:

1. Employees are required to leave their mobile phones, tablets and personal laptops at the reception desk or similar secured area and retrieve them on designated breaks or when work is finished.
2. The use of mobile phones, tablets, and personal laptops for personal activities at work is strictly prohibited and may lead to disciplinary action up to and including dismissal.
3. If the employee's family needs to contact them at work in the event of an emergency, they can contact the designated number for that employee, and the message will be relayed to the employee, either immediately or at the next convenient break depending on the urgency.
4. The same disciplinary policies apply to the use of mobile phones, tablets and other mobile devices as contained in our Internet Use Policy, and access to illegal and/or unauthorised sites is prohibited, and may lead to disciplinary action up to and including dismissal.
5. No personal mobile phones, tablets, personal laptops, and other mobile devices are allowed on/in this worksite/construction site/production floor.
6. Employees who believe that they have a valid reason to retain their mobile phone at work must seek approval from their supervisor and each request will be dealt with depending upon the individual circumstances of each employee and the nature of the request.

It is important to remain flexible in your approach to this matter and to lead by example.

Issues such as morale and individual employee performance should be considered when setting the rules at your workplace to assess the level of supervision and compliance required.

To minimise unproductive time spent by employees, employers need to keep their policies and procedures relevant and up to date with the applicable technology, and the use of Smart Phones in the workplace can then be suitably controlled.

Use of the Internet

The access that employees have to computer equipment and the way that they use it can be closely monitored and regulated by the employer to ensure that use is not abused; however, the realities are that most employers (particularly those with large organisations) are unable to physically monitor individual employee access and activities.

One option is to provide computers that can be accessed by employees for appropriate personal use during designated breaks.

Online tasks that may be considered appropriate for personal use are:

- Checking personal email accounts
- Completing internet banking
- Researching general information

Managers, supervisors, and team leaders should be responsible for ensuring their internet usage complies with company policies and is in line with the organisation's values and requirements.

Online tasks that may be considered inappropriate for personal use are:

- Illegal or unacceptable use
- Personal monetary gain
- Downloading software
- Transferring company information by any means (e.g. USB stick or hard drive)

Employees also should be advised that they are not to play, participate in or download:

- Online games
- Online gambling
- Online chat rooms
- Online travel sites
- Online Music/Video sites

If your system can accommodate it, the use of appropriate gateway software can monitor these items for you while at the same time stopping indiscriminate access and use at work.

It is also crucial to have suitable anti-virus software installed that is constantly updated and can be adjusted to meet the requirements of your business.

A survey conducted by Google found 11,000 domains hosting fake anti-virus software, accounting for half of all malware delivered by internet advertising. Wikipedia describes the following information to define malware:

> *"Malware, short for malicious (or malevolent) software, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.*
>
> *It can appear in the form of code, scripts, active content, and other software (http://en.wikipedia.org/wiki/Malware - cite_note-1). 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software (http://en.wikipedia.org/wiki/Malware - cite_note-2).*
>
> *Malware includes computer viruses, ransomware, worms, Trojan horses, rootkits, key loggers, diallers, spyware, adware, malicious BHOs, rogue security software, and other malicious programs. Many active malware threats are usually worms or Trojans rather than viruses. In law, malware is sometimes known as a computer contaminant.*
>
> *Malware is not the same as defective software, which is software that has a legitimate purpose but contains harmful bugs (https://en.wikipedia.org/wiki/Software_bug) that were not corrected before release. However, some malware is disguised as genuine software, and may come from an official company website.*
>
> *An example of this is software used for harmless purposes that is packed with additional tracking software that gathers marketing statistics.*
>
> *Malware has caused the rise in use of protective software types such as antivirus, anti-malware, and firewalls. Each of these are commonly used by personal users and corporate networks in order to stop the unauthorised access by other computer users, as well as the automated spread of malicious scripts and software."*

Unrestricted online activity at the workplace greatly increases the likelihood of phishing which is a scam in which the attacker sends an email purporting to be from a valid financial or ecommerce provider or some other organisation which is likely to get the attention of the recipient. The email often uses fear tactics in an effort to entice the intended victim into visiting a fraudulent website. Once on the website, which generally looks and feels much like the valid ecommerce/banking site, the victim is instructed to login to their account and enter sensitive financial information such as their bank PIN number, their tax file number, mother's maiden name, etc. This information is then surreptitiously sent to the attacker who then uses it to engage in credit card and bank fraud - or outright identity theft.

Most often, phishing takes the form of fraudulent emails that ask you to 'confirm your password', 'verify your account', or 'confirm your identity'.

Some simple rules to keep in mind when contacted by suspect emails are:

- No government authority will send you an email asking for private details or passwords, they would contact you or your company formally by mail
- Police do not send emails or call you to advise that a warrant or criminal procedures against you or your organisation is in place or has commenced
- Banks, the Tax Office and other financial institutions do not require you to supply passwords or personal information by email
- Emails offering to give away money or advising that you have just won a big screen TV, iPad or some other item are generally scam websites asking for your personal details to passwords etc. so that they can raid your bank accounts

With so many staff having online access in today's business environment, it is easy for employees to experience a message pop up which states that they are the 1,000,000th customer or visitor to a website and have won a prize, perhaps during a legitimate online activity or during their break. The next step is a request to follow a website or provide some basic contact details so that the prize can be collected. Once one of these websites is clicked on your system can be maliciously infiltrated.

Other sophisticated scams include the sending of invoices for services not provided and Tax Office emails asking to verify your business account details to receive an additional tax refund.

Gateway software can be constantly updated to reflect the level of access and content available within the IT system and can stop incoming messages and content which contain inappropriate material and/or wording. This type of electronic filtering can identify and implement variable levels of language and key words which will be blocked and not forwarded to the intended recipient. Filtering incoming material in this manner blocks out a great deal of spam email and inappropriate material which may be offensive and/or illegal and removes temptation from employees.

If employees receive any inappropriate material or suspect that they have been sent a phishing email, they should report the matter as soon as practicable so that it can be investigated and if possible, the gateway auditing settings updated to prevent future occurrences. Where possible conduct business with known companies that you trust and if for any reason you have concerns about them, conduct enquiries to establish their credentials.

Be particularly careful of overseas businesses seeking to purchase large orders of goods or services when the services and goods you supply are usually for domestic use and sale. A common scam in this area is for an overseas company to contact you to order a large amount of equipment for which they send a cheque for payment prior to purchase for an amount in excess of the agreed purchase price. They then request that you bank their cheque and forward to them

immediately the amount of overpayment, usually between $5,000 and $10,000. Once this is done in good faith, the initial payment cheque fails to clear the banking system and the company is left with non-payment for the goods and services and/or a net loss for the repayment of an overpayment that never existed.

Do not be rushed or pressured into making a decision or fall for high-pressure sales tactics.

Always ask for the name, identification, ABN and contact number of the person you are speaking to and who they represent. Insist on written information and quotes for work, including specific contact details about the organisation requesting the quotes. Essentially - find out exactly whom you are dealing with.

If you wish to check the details of a prospective purchaser/client, contacting the Australian Securities and Investment Commission or ASIC (on 1300 300 630 or 9911 2200) is a good place to start. Checks can also be done online if you visit http://www.asic.gov.au

Read letters and contracts carefully and seek professional advice from an accountant or solicitor if you are unsure or if significant amounts of money are involved.

Do not pay any letters of demand until their authenticity is confirmed and legal advice sought. Do not give out personal information over the telephone, such as credit card details, or the names of employees, until you have checked out the company and know that they are legitimate. Keep proper records and maintain backups and security. Poorly organised businesses are the main targets of scammers. Keep the number of people who are authorised to pay cheques and draw company funds to a minimum and ensure that access of these people is continually updated with your bank or financial institution.

Businesses who store valuable information, including credit card details, are the biggest targets for this type of operation. The advice coming from investigations into this type of incident is to check IT security and don't leave backups connected to servers. It is also recommended to keep your electronic business data backup off site and replace these copies with updated copies at appropriate intervals.

You can use online backup services to keep your business data on the net or put a backup hard drive somewhere secure such as into a bank security box. In case of physical disaster, having all your backup copies of your business data on your business premises is not a good idea.

The most important rule for staff with online access at work is to ensure that if they get an email from an unknown source or one that they believe may be suspect, it must be deleted immediately. Clicking on a website that is suspect may allow hackers to infiltrate your business systems and gain access to financial details and client and sensitive business information.

You can report a scam to SCAMWATCH (the Australian Competition and Consumer Commission) via:

- **The SCAMWATCH ACCC info centre on 1300 795 995**

Other sites for the reporting of suspicious activities are:

- **ASIC** – Australian Securities and Investment Commission (report suspicious business activity)
- **ACMA** – Australian Communications and Media Authority (report SPAM, unsolicited SMS)
- **ACCC** – Australian Competition and Consumer Commission (report scams, large amount of information on consumer awareness information)
- **APRA** – Australian Prudential Regulation Authority (oversees conduct of participants of superannuation industry)
- **AFP** - Australian Federal Police
- **AusTRAL** – Australian Transaction Reports and Analysis Centre

You can also check for recent scams and phishing activity, report a scam or phishing email or suspect transaction in Australia at www.scamwatch.gov.au.

The following clause can be used to advise employees of these matters and what will happen if breaches occur:

> *(Company name) monitors the use of (Company name) networks and may monitor selected network traffic, without notice to the user, at the request of authorised parties.*
>
> *Alleged inappropriate use of the internet will be reviewed by (Company name)'s management and/or directors on a case-by-case basis and may lead to disciplinary action up to and including dismissal.*

Breaches can be easily identified, and the offenders dealt with in accordance with the appropriate IT and disciplinary policies and procedures. It is also important when compiling these policies and procedures to include the use of personal equipment at work such as Smart Phones, tablets and laptops as most employees own and bring to work at least one of these items on a daily basis.

These items carry some specific risks such as:

- They can be logged into the employer's Wi-Fi network without trace (depending upon the sophistication of your monitoring software) and can be used to download inappropriate and/or illegal material at the employer's expense
- They can download or introduce dangerous viruses to the employer's IT system, some of which can destroy data and lock systems for ransom

- Employees can be carrying out prohibited behaviour and/or not spending their time as required by accessing online sites on their personal equipment

For these reasons it is recommended to advise staff and include in any IT or internet use policy, the following requirements:

- Use of the internet during work time must be approved by your supervisor/manager
- Under no circumstances should pornographic or inappropriate material be accessed or downloaded on the internet
- Under no circumstances should inappropriate images or content which could offend other employees be downloaded or forwarded to other employees

The policy or guidelines should also clearly state what is allowed such as:

- Permitted use of the internet, e.g. for research, ordering of supplies and equipment, company banking and business in general
- When and where access is allowed e.g. company supplied computers, privately owned computers, and phones
- What is allowed to be downloaded and what limits are applied to downloading movies and other high use material
- Where private and/or downloaded material can be stored
- The use of external USB sticks and external storage devices which may contain viruses or data that can corrupt a workplace IT system
- If or when employees can use their personal mobile phones at work and under what circumstances
- What will occur if these guidelines/policies are breached or ignored

There are numerous legal and financial risks associated with the illegal use or downloading of online material, so all users must comply with all applicable laws and regulations and must respect the legal protection provided by copyright and licenses with respect to both programs and data.

It is recommended to advise all employees that they may not upload any software licensed to their employer or data owned or licensed by their employer without explicit authorisation from the manager responsible for the software or data.

Incidents of copyright infringements and prosecution have increased in Australia where employees have purchased software and copied the programs to other computers without authority.

Most of the computer software currently available is purchased as downloadable content, and the online security associated with these products either prohibits multiuser access without payment or licencing agreements or tracks the usage so that prosecution may follow.

The following clauses may be included in your IT/internet policies to minimise the likelihood of breaches occurring:

> *(Insert employer name) will under no circumstances tolerate the making or use of unauthorised software copies by its employees, visiting staff, or contractors within our organisation.*
>
> *The processes for obtaining computer accounts within our organisation require the user to acknowledge that use of our computing facilities to breach copyright is absolutely forbidden.*
>
> *Employees, visiting staff, or contractors found to be engaging in the unauthorised copying of software will be liable to disciplinary or legal action depending upon the nature and severity of the breach.*

As stated in the sample clauses above it is important to cover all personnel who may have access to your computer software and IT systems, including contractors.

There are also significant risks for businesses that collect and store client information as part of their operations. If any of this information is leaked or used inappropriately there can be significant implications and possible legal ramifications.

For these reasons it is recommended that organisations review and revise their privacy policies and procedures to ensure that they are compatible with internet, email, and social media policies.

Users should be advised that they must not attempt to obscure the origin of any message or downloaded materials under an assumed internet address.

If your organisation uses the internet to conduct business, the staff who deal with this on a daily basis need to know exactly what they are able to do and what is not permitted as part of their daily tasks.

Another method of reducing the likelihood of internal activities assisting online hacking or phishing is to have particular databases, records or other sensitive information password protected within your own system. This introduction of security levels within the organisation can be an effective method of reducing online risk.

It should also be noted that confidentiality of business and client information applies to all forms of data collection, not just online access, and all businesses should regularly update their physical security procedures and confidentiality/privacy policies.

Case Study

A case in America found that a computer software developer had been dismissed because he had actually outsourced his daily tasks to a computer programming operation in China and spent most of his day watching cat videos and 'surfing the net'. Prior to his discovery and while under these arrangements he was recognised as one of the highest performers in the company. He earned an annual salary of $250,000 US from just one company but was involved with others and reaped several hundred thousand dollars per year. He paid the Chinese about $50,000 US per year. He was caught when his employer noticed repeated logins on the company's server from a city in China. He had supplied his log in credentials so the Chinese workers could log into the company system. It has been discovered that as he only worked two or three days a week for this initial company, he also worked in a similar capacity for two other companies.

There are other well-documented cases of employees outsourcing components of their work to overseas locations. With the exponential growth of online studies, it is currently possible to do almost any chosen course, including certain tertiary studies, online.

While these options are great for busy people who are not able to attend large periods of onsite tuition, they pose a problem when employees conduct these studies at work on work computers. The scope of mischief that employees are able to engage in has almost no limitations with the current online options available.

Case Study

Two cases uncovered by the IT section of a large local government organisation in Queensland investigating high internet usage, discovered one employee who, at the cessation of work each night before leaving, would link his computer to a network around the world and use their combined resources to send signals into outer space in an attempt to connect with extra-terrestrial beings. The second employee was uncovered using large amounts of internet resources by downloading pornographic movies. At the cessation of work each day he would log into a pornographic site, choose a range of movies, and then hit the download button. The movies would download all night and when the employee returned to work in the morning, he would save the files and hide them in document files on his computer.

These examples demonstrate the need for vigilance in supervision and diligence in the application of appropriate gateway software combined with appropriate policies, procedures, and training to minimise this type of misuse of resources and inappropriate behaviour.

Social Media

Like all new trends there is a name for the medium which has become a worldwide phenomenon so almost everything that has some form of personal or social content is referred to as 'social media'.

The problem is that the new penchant for individuals to place comments online on issues as diverse as how their pets are feeling to their most intimate moments has changed the way that people interact in a fundamental and not always positive manner.

The key vehicles used and defined as social media include:

- Podcasting
- Folksonomies
- Rating tools
- Vlogging
- Geotagging
- Aggregation
- Discussions
- Personas
- Blogs
- Tagging
- Instant messaging
- Social voting
- RSS feeds
- Reviews
- Wikis

The most common social media sites visited currently are:

1. Facebook
2. Twitter
3. Instagram
4. LinkedIn
5. Snapchat

Recent studies have identified that the most popular users of social media are young females.

Online dating has now become mainstream with almost any sector of the community catered for, including linking married people with other married people for illicit affairs.

Terrorists have used the medium to gain knowledge and promote their interests, and governments have used the same medium to prevent their effectiveness.

There are online fantasy worlds where people adopt an Avatar with their chosen persona and life circumstances and live and work in an alternate reality.

The growth in the number of people addicted to games and online activities is well-documented as are cases of people dying from 'gaming' for extended periods.

Current figures suggest that anywhere from 6 to 10 percent of online users fall into the category of addicted (ironically this information was obtained from an online search on the subject).

- In June 2018, the World Health Organisation included gaming addiction in the list of diagnosable conditions.
- They also found that over **two billion** people play video games worldwide.
- Studies have found anywhere from **1-10**% of gamers struggle with compulsive addiction issues, with the World Health Organisation finding **3-4**% in their own investigations.

Then there are the personal issues which employers and employees face every day which include the move in banking institutions and retailers away from face to face customer service and towards online activity or telephone call centres. This creates pressure on the employer to stay up to date with business trends and practices to remain competitive and employees are pushed more and more to conduct their personal business online.

It is becoming increasingly prevalent for potential employers to look at a person's social networking accounts, blogs, and so forth as they make hiring decisions. Posting inappropriate material online cannot only be difficult to remove but has the ability to restrict or adversely affect your employment prospects.

An ever-increasing number of users suffer from social media regret.

The 2017 Telstra Cyber Safety survey of 1001 Australians aged 18 to 25 found 82% of the first generation who have grown up with social media did not realise the long-term impact of their posts and 52% had regrets about things they'd posted.

The survey also found that 60% said they were more concerned now than they were as young teens about the impact their online reputations could have in the real world.

The survey showed more than half of young Australians regret posts they have made online, and although this is concerning there appears to be no downturn in the activity.

This is caused by individuals posting pictures or information through social media sites which has had an adverse outcome for them. These circumstances can include:

- Identity theft
- Lost employment opportunities
- Burglary (due to posting details of holidays and trips which identify to potential thieves that a house or office location is vacant)
- Marriage and/or relationship difficulties due to online activities and affiliations

Giving out sensitive personal information, photographs and other content continues to cause problems for employers and employees, especially if the information contains references to the place of work, work colleagues or work operations and locations.

Get Safe Online research found that 25% of registered social networking users had posted sensitive personal data about themselves on their profiles. This included details such as their phone number, home address or email address. Younger adults are even more likely to do this, with 34% of 16-24-year old's willingly posting this information. Examples ranged from posting provocative photos to photographs of teachers drinking and smoking being seen by their pupils and pupils' parents. In one recent survey, 17% of adult users said they talked to people on social networking sites that they didn't know, and 35% spoke to people who were 'friends of friends' (Adult Media Literacy Audit).

The problems that these types of online transactions and contacts can create for the employer arise where the contacts carry out online activities while at work using social media sites where there is the possibility for IT systems to be hacked and/or confidential business information leaked or stolen.

However, the main problem for business is the amount of lost or unproductive time that employees are wasting through unauthorised and unproductive online social media activities.

A simple example would be a business with 10 employees each of whom averaged 1 hour per day sending and receiving personal emails, surfing the internet, and going on to social media sites (by all accounts this is a conservative estimate). In this example, that unproductive time would amount to 10 hours per day, 50 hours per week with a total of 2600 hours over 52 weeks for the 10 employees.

To put this in perspective, a full-time employee engaged to work for a standard 38-hour week would work for 1976 hours over a 52-week period. The lost time from this example equates to approximately 1.5 full time employees' hours per year.

Looking up sports results on Monday mornings and organising the company football betting pools every week may be sanctioned within your business, but these types of online activities

can reduce productivity and create an expectation that it is accepted by management which leads to abuse. The larger the company, usually the larger the problem.

The divergence of these competing pressures arises at the workplace where the employer supplies state of the art computer equipment (usually much better than privately owned) with fast internet speed and virtually unlimited access at their workplace.

The temptation then arises to conduct their personal business while at work and this can mean spending large amounts of time on unproductive activities and lost time for the employer. The balancing act is how to provide the best possible workplace environment and IT equipment while at the same time limiting personal and private use to an acceptable and appropriate level.

Blogging

Blogging is contained in websites where users can submit their own comments and content.

Some popular websites that include photographs and blogs are:

Facebook 

Instagram 

LinkedIn 

Twitter 

Snapchat 

Employees who choose to blog must ensure that they:

- Do not blog during work hours
- Do not to use company equipment to blog
- Do not display any company trademark, logo, or copyrighted artwork
- Do not represent or imply that the blog is authored by the company
- Do not comment or display anything that may bring the company or other team members into disrepute

If employees do use company supplied computers and/or are able to have access online in out of work time while at work, some tips to be provided to employees or possibly included in your social media policy for blogging under these circumstances are:

- Have personal account settings turned on 'Private' so that only accepted friends can view your profile and blogs
- Do not accept friend requests from people you do not personally know
- Do not use company 'check in' features or comment on company promotions
- Do not post comments, 'check in', or tag other team members without their permission
- Do not make any personal comments about your employer or your workmates
- Do not post any pictures of your workplace
- Avoid 'checking in' as it can alert people to your whereabouts, potentially putting yourself or others in an unsafe situation
- Do not forget to log out of your account when you have finished using it
- If you see something that is not appropriate or has made you feel uncomfortable on another team member's blog, speak with your line manager/supervisor
- Do not post any comments or photos connecting you with your employer unless specifically authorised to do so, and only after you have obtained permission from the people involved to post their photo or details online. For example:
  - Photos of yourself or work colleagues wearing company uniform
  - Photos of yourself or work colleagues at work premises or company promotions
  - Photos or comments that others may find offensive or embarrassing
- If mentioning the company in a blog in any way, then display the following statement:

  "This blog is not sponsored or sanctioned by (Company Name). (Company name) is not responsible for the content of this blog."

Many of the issues and complaints that have arisen from the use and abuse of social media involve the theft and/or misuse of private information because unfortunately, in order to participate in some of these online activities, a certain level of personal information is required which can create opportunities for those with malicious intent.

There have been some previous cases summarised below where an employee's online comments or actions have resulted in dismissal and caused serious problems for both the employer and employee. Although these cases occurred some time ago, they were at the forefront of decisions of this type and have set the precedent for typical cases which are occurring today.

The increase of offences and dismissals which involve online activity will continue, and the best protection remains vigilance and the application of up to date and suitable policies and procedures to keep pace with the online environment.

These cases are particularly relevant to online activity and how to treat the possible misuse of online facilities and they provide some details as to what issues need to be considered when dealing with this complex employment issue.

Case Study

***Glen Stusel v Linfox Australia Pty Ltd* [2011] FWA 8444** which was upheld on Appeal. In that case, FWA ordered Linfox to reinstate Stusel after he was dismissed for making 'derogatory and/or offensive' comments about his managers on his Facebook page. Linfox attempted to rely on its induction training and employee handbook and the breach of those by Stusel by making such 'derogatory and/or offensive comments' as amounting to serious misconduct warranting summary dismissal. FWA found against Linfox and determined the termination was harsh, unjust, and unreasonable.

In his decision, Commissioner Roberts said: *"…in this current electronic age, this induction training and the handbook is not sufficient and many large companies have published detailed social media policies and have taken pains to acquaint their employees with those policies. Linfox did not."*

In the following two cases the employer had a suitable defence based on their policies and training which supported their actions and the dismissals were upheld.

Case Study

P Micallef v Holden Ltd PR900664 (25 January 2001)

In this case, Mr Micallef made an unfair dismissal claim against Holden for his termination. Micallef was terminated because he used Holden's email system to receive, maintain and then transmit emails on and via his work computer which attached and or contained pornographic material. Holden had a clear policy against such conduct in place, which Micallef acted contrary to. In addition, Holden offered training on the policy which included a video presentation. Micallef gave evidence that he paid little or no attention to the video presentation regarding it as 'another company presentation'. The Commission found against Micallef and determined that the termination was **not** harsh, unjust, or unreasonable.

The Commission said "*The Company took reasonable steps to convey the policy and its implications to the applicant and other employees. The fact that the applicant did not treat the policy presentation seriously, in my view, compounds rather than justifies his inappropriate conduct*.

Case Study

Damien O'Keefe v Williams Muirs Pty Limited trading as Troy Williams the Good Guys [2011] FWA 5311

An employee was sacked after posting an inappropriate comment on his Facebook page which contained derogatory remarks and inappropriate language. The comment was written and directed towards his employer and the operations manager after he had entered into discussions with them about pay issues. The post was made after working hours however the post was seen by 11 of his colleagues who were also his 'friends' on Facebook. His employment was terminated on the grounds of serious misconduct. The employer had an employee handbook which said: *"In communicating with other staff, customers and suppliers, employees should be courteous and polite, maintain a high level of honesty and integrity and present themselves and the business professionally. Employees will not use offensive language, resort to personal abuse or threaten or engage in physical contact."*

FWA upheld the dismissal and said: *"common sense would dictate that one could not write and therefore publish insulting and threatening comments about another employee…the fact that the comments were made on a home computer, out of work hours doesn't make a difference…as the separation between home and work is now less pronounced than it once used to be."* This case demonstrates the need to ensure that any online comments relative to employment and/or work colleagues needs to be within acceptable boundaries or severe disciplinary action may be taken and upheld.

In the two cases following, the circumstances of the online activity impacted the tribunal decisions.

Case Study

Fitzgerald v Dianna Smith trading as Escape Hair design [2011] FWAFB 1422

In this case, at first instance, Fitzgerald (the employee) lodged an unfair dismissal claim. She was terminated from her employment for multiple reasons. One of them included a Facebook posting which read:

> *"Xmas bonus alongside a job warning, followed by no holiday pay!! Whooooo!!! The hairdressing industry rocks man!!! Awesome!!!"*

FWA observed at first instance that whilst the comments were silly in the context of them being made in a public forum, it did not consider them of such a nature as to damage the employer's business. It was a 'foolish outburst' but the posting in the circumstances did not provide a valid reason for dismissal. On appeal, the Full Bench said that FWA's finding as to the Facebook post were correct, unremarkable, and open to be made.

This case reflects a possible overreaction by the employer in relation to the Facebook comments which upon examination were viewed as being relatively innocuous and not reasonable grounds for dismissal.

Case Study

Ms Tamicka Louise Dover-Ray v Real Insurance Pty Ltd [2010] FWA 8544

In this case, Dover-Ray was terminated for posting a blog on her Myspace page which criticised her employer's investigation of sexual harassment allegations made by her.

The post read:

> *"This place covers people's lives, offering to protect them when catastrophe happens and yet fails to protect the people that work for them. Chasing dollars over safety. Witch-hunting. Nothing but witch hunters. So where is the integrity of the workplace? They were absolute lies, absolute mockeries of what they stood for…This is corruption at its rawest. It is corruption at every level."*

FWA found that there was a valid reason for the termination, namely:

- The blog identified the employee by photograph and name, it was dated and referred to the recent investigation she had just gone through
- The blog was publicly accessible through a Google search
- It was of no consequence that she did not intend for the blog to be published in the general public domain, given that some of the friends she had on her Myspace page were Real Insurance employees. This meant that it could be reasonably expected that her blog, controversial as it were, would at least be circulated throughout the workplace
- The blog was in effect an attack on the integrity of the management of the employer and the criticism of corruption is of such a serious nature and degree that it cannot be brushed aside by the submission that the employer was being 'precious' by being personally offended by the blog.

What these cases also reflect is that it is crucial to manage your company's online presence and how employees access and use the online environment, and they need to be aware that comments made outside of working hours can still be used as grounds for dismissal if the comments are inappropriate.

It is also crucial that employers do not overreact to harmless comments and that fairness and equity is applied throughout the disciplinary process. Failure to adequately advise employees about their rights and responsibilities may result in the inability to adequately enforce or implement disciplinary action when breaches occur.

It is not good enough to simply have policies and procedures in place and to rely on those policies to apply disciplinary action in the workplace. Employees should be provided with copies of any applicable policies and procedures, and they should be reviewed and updated at least annually with training and communication processes in place to ensure that all staff remain aware of the policies and procedures, and any amendments that may have been made.

Attendance records for all training should be kept on file and each employee should sign that they have read and understood the policies.

Email

Email has become probably the most common form of electronic communication used by employees and its use on a daily basis has overtaken most other forms of contact.

The ability to attach documents, diagrams, plans, videos and pictures to name a few items to email communications means that complex and detailed company documentation can be transferred to clients, customers and staff quickly and efficiently at a very low cost.

While email can be an integral and useful part of an employee's daily duties, it can also be a time-wasting distraction when they are receiving and answering 'junk' emails, emails from friends and relatives and generally being diverted from their role. Many employees, if unable to access their employer's email system, conduct email transactions on their mobile phones which can also send and receive text messages while at work. It is important to advise staff that use of a company email system is at the company's discretion and that all email communications within that system belong to the employer.

The following clause can be used to explain this position:

> *E-mails received or sent from (Company name) are considered the property of the (Company name) and can be accessed by the Management of the Company at any time suitable to them.*

Proper use of email includes the following points:

- Do not send abusive or threatening emails (flame mail)
- Do not use red letters to emphasise your point
- Do not use exclamation marks or capital letters to emphasise opinions or tasks (considered to be shouting)
- Using symbols to replace crucial letters does not change the meaning of the word or its offensive intent
- Check distribution lists and recipients to ensure that the correct people receive your communications
- If you have had 3 or more emails on a topic, call the recipient
- If you receive complex or contentious content in an email that you are reluctant to respond to by return email, contact the sender and advise that "*this subject is a complex matter and I would like to discuss it with you over the telephone or at a formal meeting"*

Some useful tips when using email are:

- To stop continual disruptions, turn off the email notification function on your computer and set aside a period of time each day to sort emails and to formulate replies
- Notify friends and work colleagues who send 'junk emails' to stop sending them to your place of work and to send them to your private email address
- If you receive an email that contains inappropriate or offensive material, delete it immediately and advise the sender to stop sending this type of email
- Do not send private emails from a company system with company information or letterhead

Banning the use of email and the internet at work completely appears to have a negative impact on the workforce and can be difficult to enforce where staff have access to the internet as part of their daily duties. A limited amount of personal use of emails and the internet can be good for morale. On the other hand, excessive use of the internet by staff shows poor management and lack of motivation.

Cyber Bullying

Cyber bullying does not just apply to schoolchildren or social activities and can involve work colleagues, contractors, suppliers, and anybody else connected with the workplace.

Some of the most common forms of cyber bullying are as follows:

- **Flaming** - a brief, heated exchange that happens between two or more people using some sort of communication technology. It usually happens in a public space like chat rooms or discussion groups, rather than in private discussions like emails.
- **Harassment --** This is words, conduct, or actions being directed at a specific person with the intent to annoy, alarm, or cause emotional distress in that person. It is usually repeated messages or actions against one person.
- **Denigration --** This is information about someone that is derogatory and untrue. Online, it can be posted to a website, sent via email, or messaged to someone else. This also includes sending or sharing photos of someone that portrays them in a sexual or harmful manner. Online 'slam books' which are created in order to make fun of others are also forms of denigration.
- **Impersonation --** This is when a person pretends to be another person, usually by using the victim's password to gain access to their accounts. They then send a communication to others that is usually cruel, negative, or inappropriate posing as that person. In more extreme cases impersonation has led to someone giving out where a person lives to the wrong people, in order for them to be tracked down by said people.

- **Outing and Trickery --** Outing is sharing personal, and sometimes embarrassing, information with others who were not meant to learn that information. Trickery is tricking someone into revealing personal information and then sharing that information with others.
- **Exclusion/Ostracism --** Most people just want to be a part of a group and fit in with others. Being excluded can be seen as 'social death' and people can be excluded using online methods. The online exclusion could be being locked out of a password protected chat space or just being de-friended on Facebook.
- **Cyber Stalking --** This is stalking via the use of electronic communication using repetitive harassing and threatening communication.
- **Happy Slapping --** This method of cyber bullying is where people (usually teens) walk up and slap someone, while another person uses a phone or camera to record the incident. The video is then put on the internet for others to see even though the victim may not be aware of it.

A good rule is to only put in an email anything that you would be happy to see on the front page of your local paper, or submitted as evidence in a court of law because, quite often, that is where these communications end up.

Most business IT systems run back up systems which mean that, if required, the system can be recreated to a certain time and all emails recovered where required if an investigation is underway.

Generally, emails can be used in court as evidence and increasingly emails containing inappropriate and/or pornographic images are being used as evidence in cases of bullying and harassment and workplace discrimination.

What one person may find funny in a 'joke' email may be extremely distressing and offensive to another, so it is important to be careful of what employees send and to whom.

Case Study

A significant case determined by the Fair Work Commission involving three long serving employees who were dismissed for inappropriate use of their workplace email system, demonstrates the need to have in place, and follow, appropriate practices before dismissing employees for misconduct. The three employees, employed for 20, 14 and 12 years respectively as production workers, were confronted by the employer with evidence that they had sent pornographic images by email. All three did not deny the allegations and were subsequently summarily dismissed. They all then lodged unfair dismissal appeals, arguing they were unaware of the company's 'internet and email security framework policy' and that they had not received training specifically addressing email usage. These arguments were supported by their union organiser and site delegates but were disputed by the employer.

Fair Work Commissioner Geoff Bull determined that the employees' misuse of email did constitute a valid reason for dismissal, but a number of other factors meant the dismissals were harsh, unjust or unreasonable including:

- The trio not being given a period to digest the allegations, seek advice and respond in a "more informed manner"
- Receipt or recollection of the prior staff warnings not being put to the employees at the meetings, especially considering two of the employees had only gained email access after some of those warnings were issued
- The employer's failure to explain the lapse of time between an investigation into email misuse which finished in September 2011, and the employees' dismissal in February 2012
- None of the employer's witnesses having "any clear understanding of [the employer's] responsibilities under their Internet and Email Security Framework Policy" in failing to inform the employees, as per the policy, that their email use was being monitored
- No evidence being produced that the employees were trained on the internet and email security framework
- The consequences of the dismissal on the trio who live in a regional community and failed to gain equivalent work elsewhere

Based on this decision the three employees were reinstated to their previous positions without compensation for lost time. The comments below from Commissioner Bull further reinforce the diligence that must be applied by employers in these matters. "I would make it clear that this decision is not intended to in any way undermine an employer's right to enforce appropriate policies regarding the use of email at the workplace", Commissioner Bull stated.
"[But] it ought not to be assumed that the Tribunal will uphold an employer's right to terminate in all cases of a breach of a policy regardless of the circumstances."

Once you have identified the requirements and policy content for your organisation in relation to internet use, social media and email, each employee should be adequately informed of the policy and its content and should sign an acceptance form which contains a clause such as the one provided below. As the case above details it is necessary to regularly review, communicate and discuss these policies with your staff.

(Company Name) Technology & Internet Usage Agreement

I,_____, have received and read this copy of (Company name)'s Information Technology and Internet Usage Policy and agree to abide by all of the terms and conditions outlined therein.

I further confirm that I have been provided with a copy of (Company name)'s Information Technology and Internet Usage Policy and (Company name)'s employee manual.

Summary

It is well documented that the rate of change in the electronic medium is rapid and relentless.

This means that employers and employees need to continually evaluate their online activities to ensure they remain relevant and within acceptable guidelines.

As reinforced throughout this Guide, it is crucial to know your IT system and what is required of employees who use this system.

Many businesses put in place an IT or internet policy some years ago, but the rate of change and the addition and growth of new online activities, products and services dictates the need for a review to ensure there are proper policies, procedures and training in place to cover:

- Internet use and access
- Social media
- Email use
- Privacy issues
- Technology and devices

It is also important for employers to lead by example and deal with inappropriate behaviour or misuse of the electronic medium quickly and professionally.

The growing use of working from home and other online activities will continue to increase, and the issues concerning employees on site are just as serious for those who do some or all of their work from home or another location.

It is essential that staff performing work under these conditions are clearly advised as to their obligations in regard to:

- Online usage of company resources
- Online access and security requirements
- Use of internet by family members or others
- Online monitoring and ownership of online communications and material

Laws protecting privacy and unauthorised access to computer systems extend to personal social networking and email systems. Employers who intend to monitor communications and online activities on their business systems must ensure that their employees are notified that they do not have any expectation of privacy, and that their communications via employer equipment are being monitored, even when remotely accessed by password and/or if subsequently deleted by the employee.

The employee also has responsibilities to act in a lawful and appropriate manner while working and/or representing their employer online. Failure to do this may reduce the effectiveness of any disciplinary or remedial action taken, following a breach of these conditions.

There have been numerous cases of disciplinary action, including dismissal of employees working from home or, when supplied with a company laptop or personal computer, breaches have been discovered only to find that a family member or friend has used the equipment for private and unauthorised activities. This has resulted in damage to the business.

A 2018 Australian Bureau of Statistics report on the internet usage of Australians found that there were 14.7 million internet subscribers in Australia and 27 million mobile handsets. The biggest factor to come out of the internet usage report was the increase in interaction with businesses through social media.

- 1 in 4 Australians 'Like' or interact with a brand on Facebook on a weekly basis with 59% of people accessing social media daily
- 21% of employees access social media at work with the highest usage of 47% at lunchtime and work breaks
- 94% of users are on Facebook which remains the number one social media site

Before embarking on an online marketing strategy, it is recommended to seek professional advice on what you are trying to achieve, how you intend to achieve it, what vehicles and costs will be involved and how you intend to review and manage the results.

For example, some retail businesses have found that by discounting products online, customers are not prepared to pay higher prices in store as they quote the online price and expect the same deal wherever they shop. This can result in decreased cost margins and sales.

There are many examples of online social media campaigns dramatically affecting the business of major corporations with disastrous results and significant legal action following.

Comments made by radio announcers and media outlets are now more frequently ending up in Court as part of costly defamation actions because with the proliferation of social media and its ability to influence people's opinions on people, products and services, adverse comments or opinions reach a large audience quickly.

Individuals are not immune from these actions, and cases where individuals are sued for defamation and damages are increasing because of comments they have placed online concerning opinions about products or services and on private and personal matters.

These cases demonstrate the power that social media has and reinforces the need to understand your assets and risks in this area, and to have effective strategies and training to support your policies and procedures.

Almost weekly there is some sort of social media campaign which targets supposed injustice or promotes some new product, music or activity and the proliferation of “Fake News” has become a serious political and social issue.

Instagram influencers are now setting agendas from childcare to travel and fashion with millions of followers on some sites which gives them extraordinary social credibility with little accountability.

Online sites are recruiting people to work from home who are paid to ‘Like’ Facebook pages and online advertising campaigns to artificially inflate consumer feedback. This obviously creates opportunities for negative campaigns as well which can have a dramatic effect on online business.

These occurrences will not go away and many companies, particularly in the hospitality industry, are finding out that clients who have had, for whatever reasons, an unsatisfactory dining or accommodation experience, have posted comments online which can adversely affect their business.

There are dedicated sites online where individuals can lodge complaints against service providers and these sites have a growing impact on consumer choice. The use of social media as an advertising and/or marketing tool is growing and online links, Facebook and YouTube campaigns have been both hugely successful for some and badly damaging for others. Because of this, it is vital to align your business needs with practical business, financial and marketing plans to ensure that your expectations in this area are manageable and achievable and that your staff are fully aware of their rights and responsibilities.

There have also been some stunning success stories arising from online marketing and social media campaigns with many individuals going from obscurity to instant worldwide stardom literally overnight.

LinkedIn started as one of the world’s most popular professional networking sites and its success demonstrates that the share market is still hungry for investment in successful social media sites. Their initial projections when floated onto the New York Stock Exchange was estimated at a capital value of $3 billion dollars and after their first day of trading, were valued at over $9 billion dollars. In 2016 Microsoft purchased LinkedIn for just over $26 billion at $196 per share.

Many businesses are having enough trouble staying afloat in the current economic climate and are focussed on just trying to run their daily business the best way that they can.

Unfortunately issues such as the use and abuse of the internet, email and social media sites will not go away, and the adverse effects of the abuse can have major organisational, financial and operational impacts on the bottom line unless managed properly and professionally.

Table of Amendments

PAGE NO	AMENDMENT	NEW VERSION	DATE AMENDED
	Original release	1.0	01/11/2013
3	Addition of Smart Phones, Tablets & Mobile Devices section	2.0	01/02/2016
All	Review, update to, and addition of new statistics, blog site types, security measures, health impacts (from Intro to Summary)	2.1	30/04/2019
All	Updates and overhaul of content	2.2	22/05/2020
All	Updates and overhaul of content	2.4	06/10/2021