SOCIAL MEDIA

Social media platforms, such as LinkedIn, Facebook and Twitter offer fantastic business opportunities, enabling a firm to establish their brand image and reputation, as well as to collect intelligence on markets, customer opinions, and potential job candidates.

The use of social media also comes with various risks for businesses. You need to ensure you have policies in place so you do not fall foul of employment and data protection laws, and ensure you know how to protect your digital assets from being stolen or shared online.

In our social media guide we'll explain what you need to know about do throughout the employee life cycle:

1.During recruitment
2.During employment
3.When employees leave

1. SOCIAL MEDIA DURING RECRUITMENT

Social media sites can be great for businesses when vetting job candidates as well as to scout individuals who are suitable for a specific position, enabling a more cost effective and quicker hiring process. However, it is important that you are aware of the risks of using social media in recruitment, and how to avoid these risks.

WHAT DO YOU NEED TO KNOW?

The risks of using social media in recruitment:

DATA PROTECTION (JERSEY) 2018

- You need to notify applicants and potential recruits that vetting them through social media is part of their recruitment process and allow them to withdraw if they don't consent
- What is already recorded online can be accessed and maintained freely, however, employers have a duty to ensure that GDPR laws are followed.

REHABILITATION OF OFFENDERS

- Spent convictions or any circumstances associated with it should generally be ignored when recruiting candidates.
- However, in roles associated with the financial sector, those in public service, or roles that involve working with 'vulnerable' people such as children and elderly spent convictions may be needed to consider the candidate's suitability to the role.

DISCRIMINATION (JERSEY) LAW 2013

- Social media profiles often contain personal details such as age, religion and sexual orientation.
- If a company uses this information when deciding whether to recruit candidates they could face accusations of unlawful discrimination

HUMAN RIGHTS

- Everyone has the right to freely express their ideas and opinions on social media.
- Be mindful of this, however, if an opinion shared online has a negative impact on the business this may be considered when deciding whether to hire someone.

WHAT DO YOU NEED TO DO?

HOW TO USE SOCIAL MEDIA BACKGROUND CHECKS WITHIN ETHICAL GUIDELINES

- Use a third party to carry out social media screening - digital screening specialists can be used to ensure that only relevant personal information is taken into account when making a decision about hiring a candidate. This omits personal characteristics such as religion, age, gender or sexuality thus safeguards the business from accusations of discrimination.
- Create a clear and transparent screening policy - this should lay out how the screening process should be carried out in line with Data Protection laws.

RULES OF ENGAGEMENT AND DECISION MAKING

1. Notify applicants that you are vetting them through social media.
2. Keep accurate records of the obtained information.
3. Ensure the information is correct by validating it with the applicant and give them the right to rectify and incorrect information.
4. Information on social media may be false - so you need to rely on facts from credible sources, such as written references from previous employers.
5. Don't hire someone due to their appearance or beliefs - hire the most suitable person for the role.
6. Consider how relevant the information found online is to the role.
7. Inform all staff involved in the recruitment process of the rules of engagement and legislative requirements.

2. SOCIAL MEDIA DURING EMPLOYMENT

WHAT DO YOU NEED TO KNOW?

Social media can provide effective ways of connecting with current and prospective customers, employees and a wide range of people in a business's network. It also brings issues of compliance with data regulations and ethical guidelines.

THE RISKS OF SOCIAL MEDIA IN THE WORKPLACE

- Breaches of confidentiality - if an employee was to post sensitive information online this could be accessed by anyone in the public domain and could lead to legal issues such as GDPR breaches.
- Damage to the business's reputation - employees expressing controversial opinions or false information about the company could lead to a negative brand image.
- Cyberbullying - harassment towards employees online can lead to poor morale, loss of productivity, increased absenteeism if not dealt with correctly. Procedures dealing with bullying for the victim and perpetrator help.
- Security risks - social media platforms can be used for hackers to gather information .
- An increasing number of automated 'bots' on social media sites are fake accounts attempting to affect the perception of business image and spread fake news.

CASE STUDY

In May 2019, Danny Baker, an employee of the BBC posted a controversial 'joke' photograph of the new Royal baby. Baker was accused of being racist and was condemned by many members of the public. As Baker was a public figure, who was known to be associated with the BBC, this could not only reflect badly on himself but also the reputation of the company. As a result, Baker was sacked from the BBC.

This highlights why it is important that you understand the risks of employees using social media, and how to avoid and negative consequences.

WHAT DO YOU NEED TO DO?

SOCIAL MEDIA POLICIES

You need to have a transparent Social Media policy that outlines the rules of how everyone in the organisation should behave online. It should be:

- Easily accessible for all employees.
- Flexible and updated regularly to ensure any breaches can be responded to correctly.

A SOCIAL MEDIA POLICY SHOULD COVER

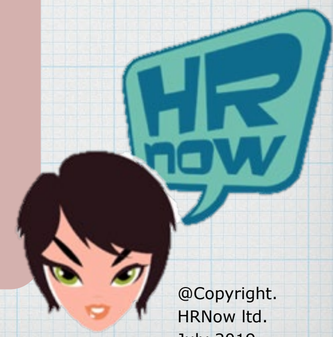
- How employees should conduct themselves online - for example, no swearing or posting negative or controversial opinions about the company or controversial topics.
- Personal use - limiting social media use at work to increase productivity.
- Consequences of misusing social media using clear examples of what would be included as misconduct - for example, disciplinary and grievance policies.
- How to protect employees from cyberbullying and the consequences for the perpetrators of bullying, such as disciplinary action.
- Security considerations - using strong passwords, protective software etc. in order to prevent social media from being hacked and information being leaked.
- Stress the importance of employees using privacy settings on social media and the potential consequences if information gets into the wrong hands.
- Explain what happens if/when employees leave in terms of LinkedIn contracts etc.

HOW TO EFFECTIVELY DEAL WITH SOCIAL MEDIA MISUSE

1. Have a clear policy.
2. Ensure everyone understands it and the consequences of misuse
3. If employees do misuse social media, deal with it quickly an in line with your stated code of misconduct.
4. Investigate thoroughly before jumping to disciplinary action.
5. If employees fail to abide, apply normal disciplinary sanctions.

EXAMPLE OF A GOOD SOCIAL MEDIA POLICY - INTEL

1. ***Disclose*** when you are posting about Intel or Intel or Intel products. If you are talking about Intel on social media, please use a disclaimer such as “all opinions are my own”. If you are leaving Intel, please update your employment information on social media sites.
2. ***Protect*** Intel. Keep Intel information confidential, do not discuss any financial, product, or legal information on social media. Don’t slam Intel or our competitors. Anything you publish must be true and not misleading. If you are unsure about whether or not to post something, err on the side of caution and do not. Our social media team can help you decide if something is permissible to post.
3. ***Use common sense.*** When you are online you are representing Intel: our people, our values. There is no room for bigotry, prejudice, misogyny, or hatred in our company or on our associated social media feeds. Stay away from saying our products are smarter/ faster/ higher-performing in your social media postings. We must use Federal Trade Commission-mandated disclaimers in all communications when benchmarking or comparing processors. Did you mess up? It happens. If you make a mistake, admit it immediately. Apologise if you need to. Be upfront, and correct the error as soon as possible.



3. PROTECTING YOUR DIGITAL ASSETS, PARTICULARLY WHEN EMPLOYEES LEAVE

Digital assets can include any account or information you use online, such as company social media and email accounts, client lists, intellectual property usernames and passwords. These assets have great value, especially to cybercriminals and rival companies, so businesses need to have processes in place to ensure digital assets are protected from theft.

WHAT DO YOU NEED TO KNOW?

Although the majority of breaches are carried out by external sources such as hackers, around 30% of data breaches are carried out by employees. The 2018 Verizon Data Breach Investigations reported that whilst some breaches were honest mistakes, most of the occurrences of data theft were motivated by financial gain and espionage.

WHAT DO YOU NEED TO DO?

FOLLOW THESE STEPS TO MITIGATE THE RISK OF YOUR DIGITAL ASSETS GOING ASTRAY

1. Clarify what information is confidential, as well as what you consider intellectual property
2. Be very clear what sources of confidential information are included, such as client and prospective client data held on social media sites like LinkedIn
3. Make sure your restrictive covenants are clear – when an employee leaves they should be in no doubt what client and prospective client data needs to remain firmly within the business
4. Don't wait until an employee resigns to clarify what is legally yours, by then it will be too late – state ownership of digital assets clearly within employment terms and conditions
5. Update your existing policies so they extend to protect your digital assets, and include any necessary wording in employment contracts, handbooks and in your social media policy. For example, intellectual property, confidential information and restrictive covenants extend to include outlook contact databases, client lists and LinkedIn contacts
6. Educate staff about your policies and what would happen should those policies be breached.
7. Ensure back up systems are in place in case a copy of assets were to be stolen - this can be simple such as using multiple external hard drives.

For further information call 747559 or contact becky@hrnow.je