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.

What 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.

Relevant laws

DATA PROTECTION (JERSEY) 2018

- Notify applicants and potential recruits that vetting them through social media is part of the recruitment process.
- Ensure that GDPR laws are followed.

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 claims of unlawful discrimination.

HUMAN RIGHTS

- Remember Freedom of Expression, but if an opinion shared online has a negative impact on the business this may be contrary to your Social Media policy and may be considered when hiring someone.

The risks

- Breaches of confidentiality - sensitive information accidentally posted online
- Damage to the business's reputation - employees expressing controversial opinions or false information
- Cyberbullying - harassment towards employees online
- Security risks - social media platforms can be used for hackers to gather information.

Protecting your digital assets

Protect 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 you need to have processes in place to ensure they are protected.

What you need to do…

Social media policies should cover:

- How employees should conduct themselves online
- Personal use - limit social media use at work to increase productivity
- Consequences of misusing social media
- How to protect against cyberbullying and the consequences for the perpetrators
- Security considerations - using strong passwords, protective software etc.
- The importance of employees using privacy settings
- Explain what happens if/when employees leave in terms of LinkedIn contacts etc.

How to 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 and in line with your stated code of misconduct
4. Take a screenshot of the post before it is taken down, as you may need this for evidence
5. Investigate thoroughly before jumping to disciplinary action
6. If employees fail to abide, apply normal disciplinary sanctions
7. This is a complicated area – if you are not sure, seek advice!

Mitigate the risk to your digital assets

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

if you'd like to know more call 747559 and let's chat!