

Social Media and Mobile Devices in Employment Policy

Policy overview

We embrace new ways of working and communicating and encourage the use of social media.

There are risks of using social media, therefore, we ensure controls are in place.

Employees should read our internal social media policy in conjunction with this policy. It gives further guidance on the use of social media websites, channels and feeds.

In this policy, social media is any online platform or app that communicates instantly or shares data in a public forum.

Social media includes social forums such as Twitter, Facebook and LinkedIn. It also covers blogs and video and image-sharing websites such as YouTube.

We are aware that there are many more examples of social media, and this is an ever-changing area.

Employees should apply these guidelines to any social media they use.

Use of social media at work

Employees can use social media at work for personal use, on our computers or devices, provided that:

- they follow our information security policy
- it does not impact on their job
- it does not interfere with other work colleagues doing their job

Employees should limit their personal use of social media to their own time. Personal time is before or after work and during rest or lunch breaks. Usually, employees must not use our computers or devices for personal use, outside of normal working hours.

Employees must limit their use of social media on their own equipment to their personal time.

Employees may use IT-approved social media websites and feeds as part of their normal work duties. The manager must agree to such usage in advance.

Social media monitoring

We reserve the right to monitor employees' use of social media on our equipment. The following are valid reasons for checking an employee's internet usage:

- spending an excessive amount of time using social media when they should be working
- spending an excessive amount of time using social media for a non-work-related activity
- breaching the rules set out in any policy
- breaching our code of conduct

Our impact assessment ensures that monitoring is necessary and proportionate. It will ensure compliance with this policy on the use of social media.

Monitoring will consist of checking

- social media sites visited
- duration of visits
- content that the employee has contributed to such sites

If we believe an employee has breached our rules, we may share the information obtained through monitoring with:

- the head of HR
- the Headteacher
- audit

We retain the information gathered through monitoring only long enough for:

- any breach of this policy to come to light
- for any investigation

Managers will only disclose information obtained through monitoring to third parties where we have to report matters to:

- a regulatory authority
- a law enforcement agency
- other professional regulatory body

Employees have several rights concerning their data. They have the right to:

- make a subject access request
- have data rectified
- have data erased in some circumstances

For more details about employees' rights, read our [GDPR policy](#).

Employees may contribute to our social media activities (for example, by running a council-owned Twitter account). Employees must be aware at all times that they are representing us.

Employees should use the same safeguards as they would with any other form of communication about us.

These safeguards include:

- the communication must have a purpose and a benefit for us
- having permission from a manager before using social media for a public campaign
- requesting a colleague to check the content before it is published

Any communications that employees make in a professional capacity through social media must not:

- bring us into disrepute, for example by referring to customers or colleagues
- make defamatory comments about individuals or other organisations or groups
- post an image that is inappropriate or links to inappropriate content
- breach confidentiality, for example by revealing information owned by us

- give away confidential information about an individual or organisation
- discuss our internal workings (such as its plans that have not been communicated to the public)
- breach copyright, for example by using someone else's images or written content without permission
- fail to acknowledge where we have permission to reproduce something
- do anything that could be considered discriminatory, bullying or harassment. For example, making offensive comments relating to any protected characteristic in law.
- use social media to bully another individual
- post an image that is discriminatory or offensive or links to such content Managers may withdraw access to social media in any case of misuse.

Personal social media

We recognise that many employees make use of social media in a personal capacity. Employees must be aware that they can damage our reputation if they are identified as being an employee.

Employees are permitted to say that they work for us. However, the employee's online profile must not contain our name (for example, a Twitter name).

Employees may discuss their work on social media (for example, giving opinions on their specialism). If they do, employees must include on their profile a statement to say, "My views do not reflect the views of my employer, Lincolnshire County Council."

Any communications that employees make in a personal capacity through social media must not:

- bring us into disrepute (for example by referring to customers, clients, members or colleagues)
- make defamatory comments about individuals or other organisations or groups
- post an image that is inappropriate or links to inappropriate content
- breach confidentiality (for example by revealing information owned by us)
- give away confidential information about an individual or organisation
- discuss our internal workings, such as plans that have not been communicated to the public
- breach copyright, for example by using someone else's images or written content without permission
- fail to acknowledge where we have permission to reproduce something
- do anything that could be considered discriminatory, bullying or harassment of someone. For example, making offensive comments relating to any protected characteristic in law.
- use social media to bully another individual
- post an image that is discriminatory or offensive or links to such content

Personal mobile devices

Employees must not excessively use personal mobile devices during work hours. Reasonable use is permitted in the event of an emergency or for exceptional personal reasons.

Ringtones can be disruptive to other work colleagues. Managers may request that personal mobile devices be set to 'silent mode' during working hours.

A manager can request that an employee turns off a mobile device during working hours if usage is unreasonable.

Social media and recruitment

Some individuals put their details on social media websites to attract prospective employers. Unless it concerns finding candidates, HR and managers must only search on social media when directly relevant to the applicant's skills or claims.

For instance:

- a prospective employee might claim that they have used social media in their previous job
- a prospective employee's social media use may be relevant to a claim made in their application. For example, if they run a blog based around a hobby mentioned in their CV.

We should not check a prospective employees' online social media activities. Conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics played a part in a recruitment decision.

For more information, read the diversity and inclusion policy.

Legal issues

We can be held legally responsible for online content published by our employees. Employees must be aware of our policy and guidelines for using social media. These policies apply whether for personal use or as a part of their job.

Consumer protection regulations forbid creating:

- fake blogs
- falsely representing oneself as a customer
- falsely advertising on social media sites

Defamation

Defamation is the act of making a statement about a person or company that is considered to harm its reputation. If the defamatory statement is written down, in print or online, it is known as libel. If it is spoken, it is known as slander.

Posting a defamatory statement online or recording it on a podcast are examples of libel.

Images

It is illegal to use graphics or photographs from the internet without permission. Employees must ensure that anyone permitting the use of an image is the original copyright owner. Employees are required to check the licensing agreement of photographs in any existing archives before use.

Employees are not to take or use any photographs of children who are under the age of 18 without permission from a parent or guardian.

Disciplinary action

All employees are required to adhere to this policy. Any breaches of this policy may lead to disciplinary action.

Severe breaches of this policy may constitute gross misconduct and lead to dismissal.