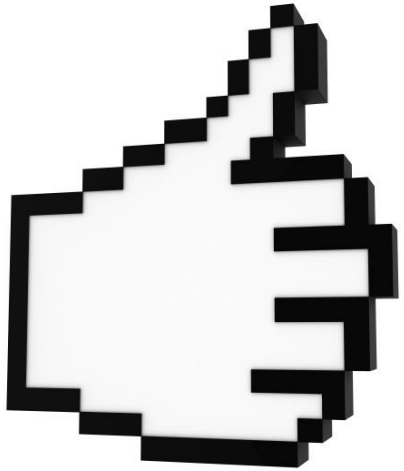
rollits

...more than a law firm



Social Media Misconduct

and related data protection issues

Ed Heppel

James Peel

Tuesday, 10 February 2015

Donna Ingleby

INTRODUCTION









Ed Heppel

SOCIAL MEDIA MISCONDUCT









Background

- Facebook (“FB”) 1.35 billion users
- LinkedIn 332 million users
- 2015 social media law still developing
- Only one EAT authority









Misuse of Social Media

- Two main types of misconduct:
  - Inappropriate behaviour exposed through social media; and
  - Derogatory comments posted on social media

Behaviour exposed through Social Media

- Misconduct evidenced by social media
- Examples
  - competing with employer; and
  - unauthorised absence
- Shark wrestling stressed employee









Derogatory comments

- About
  - Company
  - Colleagues
  - Customers
  - Suppliers
  - Non work related issues









Legal Issues Include

- Misconduct
- Discrimination
- Vicarious liability









Legal Issue 1 - Misconduct

Game Retail Limited v Laws 2014

- First EAT case
- Declined to provide guidance
- Held: Social media cases are fact sensitive
- Usual principles relating to misconduct apply









Misconduct Principles

- Reasonableness
- Fairness
- Factors
  - reasonable investigation;
  - reasonable belief;
  - GMC or misconduct.
- Range of reasonable responses
- Mitigating factors
- Alternatives to dismissal









Misconduct - Relevant Factors

- The nature of the employee's job
- The employee's seniority within the Company
- The seriousness of the alleged misconduct
- The nature of the employer's organisation
- The disclosure of any confidential information
- The risk of reputational damage to the employer
- The terms of the employer's social media policy
- The likely impact on the employee's job
- Any mitigating factors, such as the employee's service record









Misconduct – today's relevant factors

- Seriousness of alleged misconduct
- Disclosure of confidential information
- Damage to the employer's reputation
- Terms of the social media policy









Misconduct – relevant factor (1)

Seriousness of Alleged Misconduct

- Measures taken must be proportionate
- Gross misconduct or misconduct?
- Videos or photos showing violence or stealing - very serious
- Comments vary and require a measured response









Seriousness of Alleged Misconduct Case Law (1)

Young v Argos Ltd ET 2011

- Dismissed employee FB posted ex-manager is a "*chocolate teapot*"
- Y "liked" the comment
- Y commented that it had been her worst year in 15 years at Argos
- Y's dismissal unfair
- Not GMC
- No more than "*workplace gossip or routine criticism of an employer*"









Seriousness of Alleged Misconduct Case Law (2)

Blue v Foods Standards Agency 2014

- Dismissed employee No1 FB posted his manager was *"lucky a never F***ed at chair afff his heed*"
- Mr Blue "liked" the comment
- Dismissed employee No2 wrote about the manager being attacked
- Mr Blue commented *"Aye right, I wish"*
- Employer Guidance on the use of social media (primarily directed at use at work)
- Held
  - Unfair
  - £32,799.13 compensation awarded
  - Blue had exemplary employment record
  - No reason to believe employment performance would be different









Seriousness of Alleged Misconduct Case Law (3)

Rollits Case 2013

- Sacked employee posts derogatory comments about ex-employer
- Claimant posts employers are "*c*****" and *"Minnows in a lake*"
- No social media policy
- Dismissal fair
- GMC and a breach of trust and confidence









Misconduct – relevant factor (2)

Disclosure of Confidential Information

- Duty of confidentiality and fidelity
- Breach is capable of leading to dismissal
- Nature of the information will be key









Disclosure of Confidential Information Case Law

Zaver v Dorchester Hotel Ltd ET 2006

- Z employed in banqueting suite
- Z's T & Cs stressed importance of confidentiality to hotel and guests
- Stated breach could amount to GMC
- Z created internet blog with workplace concerns
- Blog mentioned colleagues and the hotel name once
- Dismissal fair
- Z understood public nature of blog
- Blog could have been a PR disaster









Misconduct – relevant factor (3)

Damage to employer's reputation

- Must be real rather than fanciful
- Access to post/video etc. relevant
- Get evidence of damage during investigatory process









Damage to Employer's reputation Case Law (1)

Taylor v Somerfield Stores Ltd ET 2007

- Manager posted YouTube video of employee in uniform
- Employee was being bashed over the head with plastic
- The video received eight hits
- Manager apologised and took the video down three days later
- Held
  - Unfair dismissal
  - Not gross misconduct
  - No evidence of damage to reputation
  - No alternatives to dismissal considered
  - No mitigating factors considered









Damage to Employer's reputation Case Law (2)

Whitham v Club 24 Limited t/a Ventura ET 2010

- Team Leader posts on FB "I work in a nursery"
- Disciplinary procedure covered outside of work actions including "posting information about your job on the internet"
- Employer relied on negative impact on relationship with VW
- Held
  - Dismissal unfair.
  - Comments relatively minor.
  - Nothing to suggest that the employer's relationship with a key client harmed.
  - "a very strange world" if a company the size of VW would terminate an agreement in these circumstances
  - No proper assessment of potential damage
- No reasonable investigation









Misconduct – relevant factor (4)

The terms of the employer's Social Media Policy

- Minimises risks associated with use of social media as it
  - Sets clear standards of acceptable behaviour
  - Puts employees on notice of potential consequences









The Terms of the Employer's Social Media Policy Case Law (1)

Preece v JD Wetherspoons plc ET 2010

- P Bar Manager
- Internet policy - disciplinary action if post lowers reputation of the organisation, staff or customers
- May 2010 P heavily verbally abused and physically threatened by two customers
- P made negative comments on FB about the customers and identified Wetherspoons
- Held
  - Could be read by wide range of people and customers
  - Could have used Wetherspoons phone hotline to air problems
  - Dismissal fair









The Terms of the Employer's Social Media Policy Case Law (2)

Crisp v Apple Retail (UK) Limited

- The Claimant's FB page open to friends only
- Posted *"once again F*** you very much work*"
- Posted two other derogatory comments about Apple products
- Dismissed for bringing the company into disrepute
- Specifically, attacking Apple's core value of protecting its image
- Social media policy emphasised Apple's image was a "core value"
- Held
  - Dismissal fair
  - Posts were not private as they could be copied
  - Apple had made clear the importance of its image









Policy Content

- The policy should include
  - Use at work - regulate, block access?
  - Consequences of defaming
  - Misuse will lead to disciplinary action and potentially dismissal
  - Examples of misconduct and gross misconduct and GMC
  - Reasons for monitoring
  - Cross reference disciplinary process, bullying and harassment and equal opportunities policy
- Review policy regularly and update if necessary
- Draw policy up in consultation with the Union or employees?









Legal Issues 2 - Harassment

- Section 26 the Equality Act 2010 defines harassment as "*unwanted conduct related to a relevant protected characteristic that has the purpose or effect of violating an individual's dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment for him or her*"; and
- The protected characteristics covered are age, disability, gender reassignment, race, religion or belief, sex and sexual orientation









Harassment - Case Law

Teggart v Teletech UK Ltd IT NI 2010

- T posted on FB "*quick question who in Teletech has [A] not tried to ****? She does get around*"
- A worked with T
- T dismissed for harassment and GMC
- Dismissal fair
- Comments vulgar and coarse
- T's intention to create a "vulgar distaste" for A









Legal Issue 3 - Vicarious Liability

- Employers are liable for acts of harassment carried out by employees in the course of their employment
- Defence if employer took all reasonable steps to prevent employee from carrying out the acts - section 109 Equality Act 2010
- One step is putting in place and communicating a social media policy and anti-harassment policy
- Case law has established that the terms “in the course of employment” is to be interpreted broadly and may include conduct that takes place outside of the work place ***Jones v Towerboot Co Limited 1997 ICR 254***









Vicarious Liability - Case Law

Otomewo v Carphone Warehouse Ltd ET 2011

- O branch manager
- Two colleagues accessed his FB account
- Posted “finally came out the closet. I am gay and proud”
- O is not gay and did not believe his colleagues thought he was
- O claimed sexual orientation harassment
- Tribunal found that harassment in accordance with s.26 EQA 2010
- O embarrassed and distressed and the comment related to sexual orientation









Vicarious Liability - Case Law

Otomewo v Carphone Warehouse Ltd ET Case no.2330554/11

- Comment had effect of violating his dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment for him
- Carphone Warehouse held vicariously liable for the harassment committed by O's colleagues
- Actions were done at work during work hours and involved dealings between staff and their manager
- Conduct clearly fell within the course of employment









Case Law Guidance - Summary

- Don’t overreact
- Apply normal principles relating to misconduct
- Have a comprehensive policy
- Train on the policy
- Apply the policy consistently









James Peel

CAN YOU SNOOP ON YOUR EMPLOYEES?

Data Protection implications of viewing an employee's social media profile

- Data Protection Act 1998 applies
- Limited specific ICO guidance in relation to monitoring social media
- May need to disclose social media in response to a subject access request









Data Protection Act 1998 - Key Terminology

- Data Controller (e.g. employer)
- Data Subject (e.g. employee)
- Processing
- Personal Data
- Sensitive Personal Data









The Data Protection Principles

1. Fair and Lawful Processing*
2. Purpose*
3. Not Excessive*
4. Accurate*
5. Length
6. Data Subject Rights*
7. Security
8. Transfers Abroad









Fair and Lawful Processing

- Identify the Data Controller and the purpose(s) for which Personal Data will be processed
- Personal Data - at least one Schedule 2 condition must apply in order to process
- Sensitive Personal Data - at least one condition from each of Schedule 2 and Schedule 3 must apply in order to process
- Consent-based conditions:
  - Schedule 2 - data subject has given consent to processing
  - Schedule 3 - data subject has given **explicit** consent to processing
  - Consent must be informed and freely given
- Alternative grounds









Risks of breaching the Data Protection Act 1998

- Information Notice
- Enforcement Notice
- Monetary Penalty Notice - up to £0.5m fine without court action
- Criminal Offences (e.g. failure to comply with a Notice)
- Liability of directors and trustees
- Compensation to individuals for damage and distress
- Prison sentences
- Reputational issues, undertakings and press releases









Case Study 1

- Bob is head of sales at Employerco
- Bob is Facebook friends with Employerco's HR Manager (Bob added the HR Manager as a friend).
- Bob calls in sick from work but the HR Manager shortly afterwards sees on Facebook a selfie posted by Bob with Justin Bieber
- It is well known that Bieber is in town for that day only
- The HR Manager forwards the photo to the HR Director









Case Study 2

- Dave is a cleaner at Employerco who enjoys Game of Thrones battle re-enactments
- Dave is on Facebook but has chosen not to add/accept any colleagues as friends
- Employerco's HR Director spots Dave 'in attire' in the park from afar. Intrigued, he adds Dave as a friend on Facebook using a fake alias and proceeds to monitor Dave's postings and view his photographs
- The HR Director then forwards the photographs of Dave's battle exploits to fellow board members









Are social media profiles private?

- Employees will likely claim they are
  - e.g. if postings can only be viewed by ‘confirmed friends’
  - But if you have 646 friends, are your postings truly private?
- There are potentially limits to an individual’s right to privacy
  - If viewing their social media profile is justified based on their role









Are social media profiles private?

- **BUT** bear the following in mind:
  - Schedule 2 & 3 conditions in DPA 1998 apply
  - Nowhere in the DPA 1998 does it state that personal information in the public domain can freely be used for any purpose
  - ICO held that a business sending its customer a YouTube link of a BBC News report about an employee accused of a crime, was “unlikely to be fair” even though there was a close business relationship with the customer









Actions for Employers

- The DPA 1998 does not prevent monitoring, but monitoring must be done in a way which is consistent with the DPA 1998
  - Employee monitoring policy
- Tell employees if you wish to impose social media rules and monitor their use of social media
  - Workers' awareness will influence their expectations
  - BUT consent must be freely given, which may not be the case in an employment environment
  - Hard to justify monitoring social media usage **outside** the workplace (although rules can be stated to apply outside of work)

Privacy Impact Assessment

Before commencing any monitoring, conduct a privacy impact assessment

- What is the purpose of the monitoring?
- Are there any less intrusive alternatives which would achieve the same goal?
  - Extra training/supervision
  - If you are concerned about staff's use of Facebook at work, you could block Facebook and ban use of smartphones in the workplace
  - Consult with trade unions or other representatives where possible









Privacy Impact Assessment

- Any adverse impact of monitoring on individuals must be justified by the benefits to the employer and others
  - Can monitoring be limited to those suspected of wrongdoing?
  - Automated monitoring rather than manual?
  - Spot checks/audit rather than continuous monitoring?
  - Any intrusion must be no more than absolutely necessary
- What obligations will arise if you monitor people?
  - DPA 1998 - e.g. notification, security and subject access
  - Article 8 European Convention on Human Rights (private and family life)
  - How will you ensure compliance with these obligations?









Privacy Impact Assessment

- See ICO's Employment Practices Code (Part 3)
  - Employers who can justify monitoring on the basis of an impact assessment will not generally need the consent of individual workers
  - BUT it must still be "fair and lawful"
  - Covert monitoring is rarely justified
  - Those involved in monitoring should be briefed on the DPA 1998 and the Code









Employee Monitoring Policy

- Policy coverage
  - Who? e.g. employees, consultants, casual workers, agency workers, interns
  - What? e.g. email, internet (including social media), telephone, CCTV
- Explain why monitoring is necessary
  - Ideally by reference to the outcome of the privacy impact assessment
- How will monitoring occur?
  - Automatic? Manual?









Employee Monitoring Policy

- State that the policy does not form part of an employee's contract of employment and can be amended at any time
- Explain the rules/standards that will be enforced by each type of monitoring
  - Otherwise, why are you monitoring them?
  - What will happen if monitoring discovers a breach?
  - Inter-relation with other policies (e.g. health and safety)
- Explain that messages may be disclosed in legal proceedings
- Encourage employees to mark personal emails as such and to ask their friends to do so too









Monitoring social media usage outside the workplace

- Harder to justify
- ICO has warned against gaining access to social media profiles by deception
  - e.g. adding an employee as a ‘friend’ using a fake identity
- In such circumstances the processing is unlikely to be “fair”
  - Position may be different if the Head of HR is expressly added as a friend
- Remember - there is no blanket permission to use publicly available personal data without the relevant individual’s consent









Monitoring social media usage outside the workplace

- It is possible to process personal data without an individual's consent, but only in limited circumstances
  - e.g. Schedule 2 condition 6 - "processing is necessary for the purposes of legitimate interests pursued by the data controller…except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject"
  - Where sensitive personal data is concerned, a non-consent based Schedule 3 condition must also apply (which are even more limited in scope)
  - Processing must also be fair and lawful
    - Social media policy
- Whether monitoring a Facebook profile is "fair, lawful and not unwarranted" will always depend on the facts of the case
  - Consider case studies









Employment Practices Code

- Data Protection Officer
- Implement, maintain and enforce policies for management and staff
- Bring monitoring to attention of staff
- Train staff and refresh
- Monitor compliance with policies and training
- Limiting exposure
- Seek advice if unsure









Social Media Implications of Subject Access Requests

- Section 7 of Data Protection Act 1998
- A data subject's right to see a copy of information held about them by a data controller
  - This could include information obtained from social media profiles
- Right is to see the information rather than the documents themselves
- Rights also to request:
  - Confirmation that the data controller is processing their data
  - Details of what the information is processed for
  - Identities of third parties who receive or may receive the information









Validity Requirements

- Generally must be in writing - includes emails and fax
- Verbal requests may be accepted if you are satisfied as to requestor's identity
- Can charge a fee of £10
- Data controllers entitled to ask for information to confirm data subject's identity and scope of request
- Must respond promptly and, in any event, within 40 days









Exemptions

- Legal professional privilege
- Confidential references given by the data controller
  - NOT confidential references *received* by the data controller
- Management planning/negotiations
  - ICO - Information used in a disciplinary matter cannot benefit from this
  - Will only apply where disclosure would cause genuine prejudice
- Exemptions are construed narrowly
  - Unlikely that any exemption will apply to an individual's social media profile (as it originated from that individual)
- No exemptions for "vexatious" requests









Information relating to third parties

- Do not disclose information relating to third party individuals unless those individuals have consented or it is reasonable to comply without their consent
  - Would include identifiable descriptions (e.g. job title) as well as names
- If neither of the above applies, you should still comply with the request as far as possible without revealing the identifying information
  - e.g. Delete or edit references to third parties









Information relating to third parties

- You may still need to disclose the identifying information if it is reasonable in the circumstances
  - May be reasonable if the requestor already knows the third party was involved (e.g. if a third party commented on the requestor's social media profile)
  - May be reasonable if the third party reference is a professional opinion









Next Steps

- Response should include a covering letter explaining the process followed and any exemptions
- Invite the data subject to revert to you with any queries
- Data subject can complain to the ICO if dissatisfied with the response
- ICO powers
  - Can order for information to be disclosed
  - Fining powers up to £500,000 per breach
- Individuals can claim compensation for damage and distress in court










any questions?

Ed Heppel

ed.heppel@rollits.com

01482 337313

James Peel

james.peel@rollits.com

01482 337312