This policy applies to all companies under Churchill Contract Services Group Holdings Ltd to include the following subsidiaries and trading names:

- Churchill Contract Services (CCS)
- Churchill Contract Services Rail (CCSR)
- Amulet (Churchill Security Solutions) (AMU)
- Churchill Environmental Services (CES)
- Churchill Contract Catering t/a Radish (RAD)
- Churchill Complete Compliance (CCC)
- Churchill Emergency Support Ambulance Services (CESAS)
- Churchill Make Ready Ambulance Services (CMRAS)

1. PURPOSE

Employees of Churchill Contract Services Group Holdings Ltd may be able to access social media services and social networking websites at work, either through company IT systems or via their own personal equipment.

This social media policy sets out the rules governing use of social media at the Churchill Group.

It explains the rules about using personal social media accounts at work and describes what staff may say about the company on their personal accounts.

Social media can bring significant benefits to the Churchill Group particularly for building relationships with current and potential customers, however, it's important that employees who use social media within the company do so in a way that enhances the company's prospects.

A misjudged status update can generate complaints or damage the company's reputation. There are also security and data protection issues to consider.

This policy explains how employees can use social media safely and effectively. It applies to all employees and it is essential that all employees read and comply with this policy and the company's associated policies on data protection, equal opportunities and disciplinary.

2. SCOPE

This policy applies to all staff, contractors and volunteers at the Churchill Group who use social media while working — no matter whether for business or personal reasons.

It applies no matter whether that social media use takes place on company premises, while travelling for business or while working from home.

The world of electronic and social media is constantly developing and changing and as a consequence new social media websites and mediums are constantlydeveloping.

Social media sites and services include (but are not limited to):

- Popular social networks like **Twitter** and **Facebook**
- Online review websites like **Reevoo** and **Trustpilot**
- Sharing and discussion sites like **Delicious** and **Reddit**

- Photographic social networks like **Flickr** and **Instagram**
- Question and answer social networks like **Quora** and **Yahoo Answers**
- Professional social networks like **LinkedIn** and **Sunzu**
- and any other similar sites.

In addition, the range of different electronic devices available for communication is constantly developing. Such devices would include computers, laptops, handheld devices, mobile phones, tablets etc.

3. DEFINITION

Software	The programs and other operating information used by a computer / Electronic device.
Social Media	Websites and applications that enable users to create and share content or to participate in social networking.
Electronic Device	An electronic device is any device capable of making or transmitting still or moving photographs, video recordings, or images of any kind; any device capable of creating, transmitting, or receiving text or data; and any device capable of receiving, transmitting, or recording sound.

4. RESPONSIBILITIES

Directors	• To ensure this policy is suitable and applied to Churchill Group Company Operations and routinely reviewed as and when required;
Operational Managers	• Responsible for ensuring that this Policy and associated guidance is implemented and adhered to in their respective business units; • Any concerns raised by customers, employees, contractors or members of public relating to use of social media by Churchill employees/contractors are suitably addressed.
Account Managers and those with management and supervisory responsibility for others	• Have the responsibility to direct, guide and support the implementation of this Policy; • Seek guidance from their line manager or the HR department if in doubt of any aspect relating to this Policy.
HR Department	• Ensure this policy is routinely reviewed • Have responsibility to support and guide the implementation of this Policy. • Assist in providing suitable advice on any matters relating to any this policy; • Ensure any incidents relating to incorrect use of social media are suitably investigated
IT Department	• Suitably monitor the incorrect use of company IT equipment relating to use of Social Media.
HSEQ Department	• Ensure any incidents relating to incorrect use of social media are suitably investigated
Subcontractors	• Ensure all aspects of this policy are adhered to.

5. IMPLEMENTATION OF THE POLICY

5.1 General Guidelines

Churchill recognises that social media offers a platform for the company to perform marketing; stay connected with customers and build its profile online.

The company also believes its staff should be involved in industry conversations on social networks. Social media is an excellent way for employees to make useful connections, share ideas and shape discussions.

The company therefore encourages employees to use social media to support the company's goals and objectives.

- Know the social network. Employees should spend time becoming familiar with the social network before contributing. It's important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates.
- If unsure, don't post it. Staff should remain on the side of caution when posting to social networks. If an employee feels an update or message might cause complaints or offence, or be otherwise unsuitable — they should not post it. Staff members can always consult their line manager for advice.
- **Be thoughtful and polite.** Many social media users have got into trouble with their compny or the law, simply by failing to observe basic good manners online. Employees should adopt the same level of courtesy used when communicating via email.
- **Look out for security threats.** Staff members should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. Further details below.
- **Keep personal use reasonable.** Although the company believes that having employees who are active on social media can be valuable both to those employees and to the business, staff should exercise restraint in how much personal use of social media they make during working hours.
- **Don't make promises without checking.** Some social networks are very public, so employees should not make any commitments or promises on behalf of Churchill without checking that the company can deliver on the promises.
- **Handle complex queries via other channels.** Social networks are not a good place to resolve complicated enquiries and customer issues. Once a customer has made contact, employees should handle further communications via the most appropriate channel — usually by company email or telephone.

Use of company social media accounts owned and run by the company.

Sections 5.2 – 5.5 of the social media policy covers all use of social media accounts **owned and run by the company.**

5.2 Authorised Users

Only people who have been authorised to use the company's social networking accounts may do so. Authorisation is usually provided by the HR Director or Managing Director. It is typically granted when social media-related tasks form a core part of an employee's job. Allowing only designated people to use the accounts ensures the company's social media presence is consistent andcohesive.

5.3 Creating Social Media Accounts

New social media accounts in the company's name must not be created unless approved by HR Director or Managing Director

The company operates its social media presence in line with a strategy that focuses on the most- appropriate social networks, given available resources.

If there is a case to be made for opening a new account, employees should raise this with Operations Director or Function Director

5.4 Purpose of Company Social Media Accounts

Churchill's social media accounts may be used for many different purposes.

In general, employees should only post updates, messages or otherwise use these accounts when that use is clearly in line with the company's overallobjectives.

For instance, employees may use company social media accounts to: Respond to

- customer enquiries and requests for help.
- Share blog posts, articles and other content created by the company.
- Share insightful articles, videos, media and other content relevant to the business, but created by others.
- Provide fans or followers with an insight into what goes on at the company. Promote
- marketing campaigns and special offers.
- Support new product launches and other initiatives.
- Social media is a powerful tool that changes quickly. Employees are encouraged to think of new ways to use it, and to put those ideas to their line manager.

5.5 Inappropriate Content and Uses

Company social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the company into disrepute.

When sharing an interesting blog post, article or piece of content, employees should always review the content thoroughly, and should not post a link based solely on a headline.

Further guidelines can be found below.

5.6 Acceptable Use

- Employees may use their personal social media accounts for work-related purposes during regular hours, but must ensure this is for a specific reason (e.g. competitor research). Social media should not affect the ability of employees to perform their regular duties.
- Use of social media accounts for non-work purposes is restricted to non-work times, such as breaks and during lunch.

5.7 Talking about the Company

- Employees should ensure it is clear that their social media account does not represent Churchill's views or opinions.
- Staff may wish to include a disclaimer in social media profiles: *'The views expressed are my own and do not reflect the views of my employer.'*

5.8 Safe, Responsible Social Media use

The rules in this section apply to:

- Any employees using company social media accounts.
- Employees using personal social media accounts during company time.

Users must not:

- Create or transmit material that might be defamatory or incur liability for the company. Post messages,
- status updates or links to material or content that is inappropriate.
  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.
- This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Use social media for any illegal or criminal activities.
- Send offensive or harassing material to others via social media.
- Broadcast unsolicited views on social, political, religious or other non-business related matters.
- Send or post messages or material that could damage the Churchill Group's image or reputation.
- Interact with the Churchill Group's competitors in any ways which could be interpreted as being offensive, disrespectful or rude. (Communication with direct competitors should be kept to a minimum.)
- Discuss colleagues, competitors, customers or suppliers without their approval. Post, upload,
- forward or link to spam, junk email or chain emails and messages.
- Personally 'connect' or 'link' with Clients or Members of the public on client sites i.e. Students.

No work email addresses should be registered on social media sites unless such sites are being used for legitimate company activity and you have approval by the Head of IT or Director of HR to register the company email on such a site.

It is essential that at no time any company trade secrets or confidential information relating to the company and or its employees is disclosed on social media sites or generally.

Any employees making use of social media for approved company use should ensure they do not breach any copy right or intellectual property rights of others.

Further, where social media sites are used for company purposes then any contacts must be stored on the company computer system and not simply on the social media site. Such contacts will become the property of the company.

5.9 Copyright

The Churchill Group respects and operates within copyright laws. Users may not use social media to:

- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
- If staff wish to share content published on another website, they are free to do so if that website has obvious sharing buttons or functions on it.
- Share links to illegal copies of music, films, games or other software.

5.10 Security & Data Protection

Employees should be aware of the security and data protection issues that can arise from using social networks.

Maintain confidentiality

Users must not:

- Share or link to any content or information owned by the company that could be considered confidential or commercially sensitive. This might include sales figures, details of key customers, or information about future strategy or marketing campaigns.
- Share or link to any content or information owned by another company or person that could be considered confidential or commercially sensitive.
  For example, if a competitor's marketing strategy was leaked online, employees of the Churchill Group should not mention it on social media.
- Share or link to data in any way that could breach the company's data protection policy.

Protect social accounts

- Company social media accounts should be protected by strong passwords that are changed regularly and shared only with authorised users.
- Wherever possible, employees should use two-factor authentication (often called mobile phone verification) to safeguard company accounts.
- Staff must not use a new piece of software, app or service with any of the company's social media accounts without receiving written approval from their Director.

Avoid social media scams

- Staff should watch for phishing attempts, where scammers may attempt to use deception to obtain information relating to either the company or its customers.
- Employees should never reveal sensitive details through social media channels. Customer identities must always be verified in the usual way before any account information is shared or discussed.
- Employees should avoid clicking links in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague- sounding direct messages.

5.11 Monitoring Social Media Use

- Company IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate business use.
- The company therefore reserves the right to monitor how social networks are used and accessed through these resources.

Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all data relating to social networks written, sent or received through the company's computer systems is part of official Churchill Group records.

The company can be legally compelled to show that information to law enforcement agencies or other parties.

Employees must understand the computer system and other electronic systems provided are owned by the company and the company has the absolute right to monitor the employees use of the internet and e-mail system and communications on work provided equipment.

5.12 Email

E-mail can of course be used for legitimate organisational activity. In using e-mail, it should be used only as necessary. In addition, appropriate consideration should be given to the standard of presentation, who the recipients should be, and any security related matters.

In addition, it must be recognised that e-mails can become legally disclosable and so become evidence in legal proceedings.

It is of paramount importance that employees do not send offensive or demeaning messages. It is equally the case messages that would breach the employer's Equal Opportunity policy should not be sent.

Where an employee receives inappropriate or offensive messages then this should be reported to the company.

In terms of personal e-mails, while this is not to be encouraged the employer recognises that there will be a certain amount of personal use of the e-mail system. This however should be kept to a minimal level.

Employees should not send or circulate any offensive or inappropriate material. Employees should discourage others from sending such material to them.

5.13 Internet Use

Employees should not access the internet during works time using the company's computer system or any mobile or handheld or other devices unless it is for legitimate organisational related matters.

Great care should be undertaken in down loading any material from the internet due to the problem of viruses. The down loading of such material is only allowed where it is for a legitimate organisational matter.

It is entirely forbidden to use the company's computer system or any mobile or handheld devices at any time to view or attempt to view pornographic material. If this rule is breached, then it may result in dismissal.

Employees are able to use company provided computers or devices to access the internet during breaks and just before the start or just after the completion of working hours subject to such usage being limited to a reasonable period of time.

5.14 Security

Employees should take care to ensure the security of their computer and any passwords they use. They should not disclose any passwords they use to any other employees or attempt to gain access to anyone else's computer system or electronic information where they do not have the relevant authority.

Employees should ensure they use any company antivirus software issued and or follow any anti-virus procedures issued by the employer. In addition, employees must not breach or attempt to breach the employer's firewall.

5.15 Software

Employees must not load software on to their computer or any other company electronic devices unless it is work related and they have permission to do so.

Potential sanctions

Knowingly breaching this **Electronic and Social Media Policy** is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

Where comments or behaviour made via social media, email, phone, text or other electronic/communication means about the company, work colleagues, clients, or those associated with the company, which are offensive, discriminatory, or defamatory or that may result in reputational damage for the company may give rise to disciplinary action, even if the comments or behaviour are not made using company equipment or during works time.

If they have some relation to work by the company name being linked to the comments/behaviour, or some relation to work by nature of the contents of the comment or nature of the conduct, or they are about or target someone associated with the company, then such conduct may well be sufficient for the matter to be viewed as work related and so a disciplinary matter.

5.16 Incident Reporting

Employees must report any incidents of known misuse of company equipment or incidents involving the misuse of social media, regardless of whether this has amounted to a formal complaint or not, to their line manager immediately.

6. ASSOCIATED DOCUMENTS

Associated documents to be used with this policy include:

- CG-P-03 Confidentiality Policy. CG-
- P-07 Data Protection Policy.
- CG-P-09 Disciplinary Policy.
- CG-P-14 Equal Opportunities Policy. CG-P-
- 22 Harassment & Bullying Policy. CG-
- P-24 IT and Information Policy.
- CG-P-26 Laptop Policy.
- CG-P-27 Mobile Phone Policy.
- CG-P-34 Safeguarding Policy.
- CG-P-43 Use of Information Systems Policy.
- CG-P-45 Whistle Blowing Policy.
- CG-P-55 Electronic Hand Held Devices. CG-
- P-64 Information Security Policy.

7. APPLICABLE LEGISLATION

The main legislation applicable to this Policy includes:

- Defamation Act
- Copyright, Designs and Patents Act
- Communications Act
- Protection from Harassment Act Data
- Protection Act
- Equality Act

This policy will be formally reviewed annually and updated as required. Signed on

behalf of Churchill Contract Services Group Holdings Ltd.

J.M. Briggs, Group Managing Director

Date: July 2018