

IT POLICY

This is the Company's policy on the use of its computers and mobile devices and access to the telephone, email, internet and intranet systems or any other similar system used by the

Company. Our IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.

This policy should be read in conjunction with the All3Media Group's data protection policies and procedures, including All3Media's Data Security Policy, Data Management Policy and Data Breach Protocol. These data protection policies contain further information about the Company's policies regarding the use of its IT systems and the standards you must observe when using these systems, the circumstances in which your use will be monitored and the action that the Company will take in respect of breaches.

This policy applies to anyone who has access to the Group's IT and communication systems.

Computer, email, internet and intranet usage is strictly limited to business purposes and an occasional and reasonable level of personal use, subject to conditions (see 'Mobile telephone usage and personal use of IT equipment' below). However, using the Company's computers, networks or any other storage media for any of the following are strictly prohibited and will usually amount to gross misconduct (please note that this list is not exhaustive):

- The viewing, transmitting, downloading and installing of:
 - o illegal, offensive, discriminatory, obscene, immoral or indecent material or any material in bad taste. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any reasonable person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy;
 - o pornographic material (that is, writing, pictures, films and video or audio clips of a sexually explicit or arousing nature);
 - o criminal material or material which is liable to cause embarrassment to us, our employees, workers or contractors or to our clients;
 - o a false and defamatory statement about any person or organisation;
 - o material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy, Prevention of Sexual Harassment or our Anti-Harassment and Bullying Policy). If you witness or are a victim to any form of bullying, intimidation, discrimination, harassment, sexual harassment or victimisation being completed online or by email or otherwise on the Company's IT systems by a colleague, during either work or leisure time, you should report this to your Manager or HR;
 - o unauthorised software;
 - o any other statement which is likely to create any criminal or civil liability (for you or us).
- The creation or transmission of material which is designed or is likely to cause annoyance, inconvenience or needless anxiety. This includes defamatory material;
- The duplication and/or distribution of any copyrighted material, including music, film,

software and/or any other literary and artistic works. This includes software licensed by the Company and the transmission of material such that this infringes the intellectual property rights or copyright of another person or organisation. It is the policy of the Company to comply with intellectual property law including copyright law;

- The excessive use of personal 'chat' programs or social networking sites such as but not limited to Facebook, WhatsApp, Snapchat, Instagram or X. Sending or receiving Personally Identifiable Information (PII) and/or confidential information via these programs is strictly prohibited. Excessive use would be use that interferes with the proper performance of your duties. For further information please refer to our Social Media Policy;
- Gaining unauthorised access to restricted areas of the network, password protected

documents, another employee's e-mail, voicemail or fax information;

- Hacking into unauthorised areas, altering system settings or making any changes to computers and systems that renders them unusable by others;
- Carrying out any activity which could have the effect or potential effect of damaging the reputation, credibility and/or business interests of the Company or the Group;
- Sending confidential information belonging to the Company or the Group and others including its staff, customers and suppliers (except as authorised in the proper performance of your duties) and/or
- Deliberate activities with any of the following characteristics:
 - o Wasting staff effort or networked resources;
 - o Corrupting or destroying other users' data;
 - o Violating the privacy of other users; and/or
 - o Disrupting the work of other users.

Any such action will be treated very seriously and may result in summary dismissal/the termination of your engagement.

The Company reserves the right to delete from its computer systems and storage media, or restrict access to, any seemingly unauthorised copies of copyrighted materials it may find, and any seemingly unauthorised personal data it may find at any time and without notice.

You are responsible for the security of your device(s) (desktop computer/laptop, mobile etc.) allocated to or used by you. You must log out or lock all devices if left unattended and log out and shut down your computer at the end of each working day. You must follow the password/passcode recommendations as detailed in the Data Security Policy, and keep portable devices with you or safely stored when away from the office. You must only log on to our systems using your own username and password and must not use another person's username and password or allow anyone else to log on using your username and password. In addition, you must not allow the device(s) to be used by an unauthorised person. If you suspect your device has been compromised or infected by a virus or similar, please inform your IT Support team immediately.

Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting your IT support team.

For further information about the Company's rules regarding downloading/installing software and external devices please refer to the Data Security Policy.

If using your own/personal device to process or store company data, you must follow the security

recommendations in the preceding paragraph and as set out in the Data Security Policy, together with any other instructions given to you from time to time by the Company. In addition, you must ensure the device is running licensed software with all supplier/manufacturer recommended security patches installed together with up-to-date anti-virus software.

Should you need, in the proper course of your duties, to download, upload, transmit, make available or otherwise distribute copyrighted material and/or to view, transmit, download and install offensive, obscene or indecent material then you are required to obtain prior express authorisation from either the Company's CEO, COO or MD (as appropriate) or Head of Business Affairs and you must inform the Group Technical Operations Director in writing prior to doing so.

Every employee and individual engaged to carry out work for the Company must comply with this policy and the terms of any regulations, policies and/or procedures which may be issued by the Company from time to time regarding use and access to any part of the Company's electronic communications or data storage systems. Any misuse of the Company's systems and breach of any relevant policy will be taken extremely seriously and for employees will be

dealt with under the Disciplinary Procedure, and disciplinary action may be taken, up to and including summary dismissal if appropriate in serious cases. In the case of individuals who are not employees, your engagement may be terminated forthwith. Misuse of the internet can in some cases be a criminal offence.

Systems and Data Security

You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

You must not download or install software from external sources without prior authorisation from your IT support team. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from your IT support team.

You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

2.3 Phone Usage and Email Etiquette

Mobile telephone usage and personal use of the IT systems

If you should need to make personal calls, use the Internet for personal use and/or send personal emails it is requested that you keep this to a minimum and that this type of usage should not affect the proper performance of your duties. You should be aware that the Company reserves the right to monitor all internal and external electronic and telephone communications passing through its networks and systems, which would include personal use (see 'Monitoring' below and the Company's Data Security Policy and Data Management Policy for further information).

Please note that personal use is a privilege and not a right and it must not be overused or abused. The Company may withdraw permission for it at any time or restrict access at its discretion. Any

personal use must meet the following conditions:

- (a) it must be minimal and take place substantially outside of normal working hours (that is, during your lunch break, and before or after work);
- (b) it should be made clear in the body of the email or its subject header that it is personal;
- (c) it must not affect your work or interfere with the business or the proper performance of your duties;
- (d) it must not commit us to any costs; and
- (e) it must comply with this policy and the Company's other policies, including but not limited to, the Equal Opportunities Policy, Prevention of Sexual Harassment Policy, Anti-Harassment and Bullying Policy and Data Security Policy.

Misuse or excessive personal use of our telephone or email system or the internet will be dealt with under our Disciplinary Procedure, and may result in disciplinary action being taken, up to and including summary dismissal or the termination of your engagement.

We recognise that certain roles need to view content as part of their responsibilities and recommend whenever possible/practical this is carried out using Wi-Fi rather than mobile data connections. Downloading or streaming video content etc. for personal use should only be done over Wi-Fi and is subject to reasonable usage. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

Be aware of data roaming charges that apply, especially if abroad. Contact your IT Support team in advance of travelling to identify the most effective solution.

You should take care of mobile phones and ensure they are secure at all times. In the event that one is stolen you should notify your Manager and your IT support team immediately to report the theft as per the Data Breach Protocol. In the absence of your Manager, you should take all reasonable steps to report the matter promptly so that steps can be taken to disconnect the phone. For further information about the Company's rules regarding mobile phone use please refer to the Data Security Policy.

Mobile phones whilst driving

It is illegal to hold a phone (or similar handheld device) or sat nav while driving or riding a motorcycle. Please see current legislation for details of potential penalty points, fines or loss of licence if you use a hand-held phone when driving. If the matter goes to Court, the offender could face a greater fine and discretionary disqualification.

The law still also applies to you if you're: stopped at traffic lights, queuing in traffic and/or supervising a learner driver.

In addition, research has shown that hands-free calls are also distracting, and drivers should be aware that they still risk prosecution for failing to have proper control of their vehicle, for careless or even reckless driving if use of a phone affects their driving in this way.

As a result, all individuals are prohibited from taking or making telephone calls using, or from otherwise using (for example, texting from), a hand-held phone or similar device whilst driving a company vehicle or their own vehicle on company business. The Company may discipline anyone

who acts in breach of this policy and any penalties/fines incurred for driving offences as a result will be their responsibility to pay.

In addition, from a health and safety point of view, you should not use the hands-free kit where such use would result in you being distracted from your driving and thus your driving being careless or reckless. Once again, the Company may discipline anyone who acts in breach of this policy.

Sharing of confidential information and personal data

Personal Data must never be transferred to any third party unless it is in accordance with the “Data Management Policy”.

The following measures must be taken in order to prevent Group information being accidentally included in documents believed to be blank templates:

- You must double check all template documents (including, but not limited to, contributor questionnaires and log sheets) prior to emailing or otherwise distributing them to third parties such as potential contributors to ensure that they are clean templates; and
- You should always save template documents as “read only”.

Requests from authoritative or administrative bodies

If you receive a written request purporting to be from an authoritative or administrative body (such as the police) to disclose Group information, you must immediately refer the request to your legal and business affairs team who must liaise with, and follow the instructions of, the All3Media Group General Counsel prior to responding to such request. In respect of any

requests purporting to be from an authoritative or administrative body you must keep a written record of any actions taken to and/or responses made to such requests.

You must never comply with an oral request for Group information from anyone without prior express written consent from the All3Media Group General Counsel.

Monitoring of systems and equipment

You should be aware of the risks of importing viruses and other such malicious programs onto company IT systems. Your IT Support team will ensure all software is up to date with the latest security patches and install anti-virus programmes on company devices. If you are using your own device to access or store company data and or connect to company networks or systems, it is your responsibility to ensure all security patches and anti-virus programmes are up to date.

We monitor e-mails under the Data Security Policy and Data Management Policy passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious report it immediately to your IT Support team and do not reply to it, open any attachments or click any links in it.

You must also be particularly vigilant if you use our IT equipment outside the workplace and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and subject to data protection legislation. Such information must be treated with extreme care and in accordance with

our Data Protection Policy. You must inform your IT support team immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise.

Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes. We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

- To monitor whether use of the email system or the internet is legitimate and in accordance with this policy.
- To find lost messages or to retrieve messages lost due to computer failure.
- To assist in the investigation of alleged wrongdoing.
- To comply with any legal obligation.
- To ensure the protection of our confidential information.

Employees and individuals engaged by the Company who are found to be misusing Company and/or Group systems or equipment may be subject to the Company's Disciplinary Procedure, which may lead to dismissal or the termination of their engagement with the Company (for non-employees). Where evidence of a criminal activity is detected, the matter may be referred to the police.

For further information regarding monitoring please refer to the Company's Data Security Policy and Data Management Policy.

Email Etiquette

Email lacks the cues and context of face-to-face or telephone conversations such as body

language, facial expressions or hearing tone of voice. Therefore, tone and intent can easily be misinterpreted, and remarks misunderstood. Additionally, email is a permanent record - what you say and how you say it is not retractable. Below are some tips/thoughts that should be considered when emailing a colleague:

- Does the wording represent what you would like to convey in the manner in which it is meant?
- Avoid the use of '!' and capital letters particularly in the body of an email as these can be interpreted as shouting or being aggressive.
- How well do you know the recipient?

Other points to bear in mind:

Use of the content

- You should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, sexual harassment, defamation, breach of confidentiality or breach of contract.
- An email may be forwarded to others or copied, including to a public bulletin board.
- Ask yourself if there is any section you would not wish to be identified with - if it were

removed from the surrounding context.

Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. You should not:

- (a) send or forward private e-mails at work which you would not want a third party to read;
- (b) send or forward chain mail, junk mail, cartoons, jokes or gossip;
- (c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them;
- (d) sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;
- (e) download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear that the owner of such works allows this; or
- (f) send confidential messages via email or the internet, or by other means of external communication which are known not to be secure.

Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business unless you have authority from the Company to do so (and in such circumstances please make it clear that such communication is on behalf of the Company). Only use the e-mail account we have provided for you.

If you receive an email in error you should inform the sender.

Spell and use grammar with care as spelling and grammar mistakes distract from the content and can leave your recipients with the impression that you rushed your message. Email reveals a great deal about the sender: if an email is written carelessly, the recipient wonders if the writer is careless in other matters as well. Proofread content for mistakes a spell-checker may not catch.

Choose your Subject Line carefully. A well-chosen subject line makes it easier to find the email weeks later when you and your recipient have forgotten the subject line but remembered the topic.

Respect the privacy of others. Careless use of others' email addresses could result in their emails getting spammed or other unwanted email.

You must not send messages from another person's email address (unless authorised) or under an assumed name.

Contract validity and other legal issues

- Contracts which bind the Company can be created, amended or cancelled by email. You should not agree to terms or enter into contractual arrangements or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter. Email can also be used as evidence in the event of legal proceedings and disputes.
- Messages sent over the e-mail system, both internally and externally, can give rise to legal action against the Company. You must not send abusive, obscene, discriminatory, harassing, derogatory, defamatory or otherwise inappropriate emails. You are also reminded that messages are disclosable in any legal action commenced against the Company relevant to the issues set out in the e-mail. Deletion from your inbox does not mean that the email cannot be recovered for the purposes of disclosure.