IT Acceptable Use Policy

Acceptable Use framework for information Services and Security at Mediahuis

Version Control

Version	Status	Date	Revision
0.1	Concept	30 October 2019	First approved draft

Distribution List

Name	Role	Signature	Version	Date
Henry Minogue	Chief Information Officer		0.1	30 October, 2019
Brendan Darcy	Group Head of Audit, Risk and Compliance		0.1	30 October, 2019
Edward McCann	Deputy Publisher		0.1	30 October, 2019
Paul Vickers	Chief Legal Officer		0.1	30 October, 2019
Fergus Foody	Legal Manager – Editorial		0.1	30 October, 2019

MEDIAHUIS

Contents

1 Introduction

1.1 Background

1.1.1 The Information Technology Acceptable Use Policy has been implemented to assist in ensuring the effective governance of Independent News and Media's IT systems and information.

1.1.2 If you have any queries about your use of T& Services generally then you can contact the T&I Service Desk as follows:

- Email – servicedesk@independent.ie
- Telephone – 01 7055530

1.2 Purpose

1.2.1 The purpose of this policy is to ensure that all Users use the Company's Information Technology (IT) facilities in an effective, efficient, legal and ethical manner and to ensure they understand the Company position in relation to the control and use of such facilities. Employees are defined as anyone working for the Company, whether permanent, temporary, casual, part-time or fixed-term contract and to individuals such as agency staff and consultants and volunteers who are not our employees, but who work at Independent News and Media

1.3 Scope

1.3.1 This policy applies to all Users utilising the Independent News and Media network, company owned data, software, hardware, laptops, communication devices, portable media devices and any other matter contained herein; all forms of electronic communications, internally and externally, and includes all e-mails, company provided collaboration tools (Skype for Business & Microsoft Teams), faxes, SMS messages and voice communications.

1.4 Applicability or Responsibilities

1.4.1 This policy is effective on a global basis and applies to all Independent News and Media Group Companies and Users, subject to local jurisdictional legislative requirements. This policy is the authoritative direction on this matter and supersedes any previous policy or directive.

1.4.2 The Company considers any breach of this policy and/or misuse of the Company's IT facilities, whether inadvertent or deliberate as a serious matter which could lead to disciplinary action being taken and/or IT facilities being withdrawn. Where appropriate to do so, legal action or notification to enforcement authorities may be undertaken by the Company.

2 Policy

2.1 Use of IT Resources

2.1.1 Use of the IT facilities includes (but is not limited to); the use of data/programs stored on the Company's computer systems, data/programs stored on magnetic tape, memory key, CD ROM or other storage media that is owned and/or maintained by the Company, and any Company data/programs stored on media that is not Company-owned. It further includes all internal and external correspondence using the IT facilities whether by way of e-mail, company provided collaboration tools (Skype for Business & Microsoft Teams) or other means.

2.1.2 The Company is committed to ensuring that its workplaces are free from unlawful discrimination. The IT facilities provided by the Company are intended to promote effective communication for the Company and its customers on business matters. It will not tolerate any use of its computer systems which creates a hostile or offensive work environment, or is discriminatory against or offensive to any individual or group.

2.1.3 Reasonable personal use of the IT facilities is permitted but employees must ensure that their work performance, in terms of productivity or otherwise, is not affected.

2.1.4 The Company reserves the right to temporarily or permanently limit, withdraw or restrict the use of, or access to any IT facilities if they are used in an inappropriate manner.

2.2 The Computer System – Software

2.2.1 All software and system modifications used on any of the Company's computers must be approved in advance by INM IT. Only personnel authorised by INM IT as part of their employment role may load software onto any of the Company's computers, connect any hardware or other equipment to any such computers or move or change any such computer equipment.

2.2.2 Users must not make any copies of software except where this is expressly permitted by the copyright owner or as permitted by law. It is not permitted to use software for which the Company does not own a current user licence.

2.2.3 If you have unlicensed software on a machine for which you are responsible, you must remove the installation immediately or notify the IT Helpdesk to assist with its removal. This applies whether or not you actually use the software. If you are unsure whether you have a licence for a particular package, check with INM IT. Where you are supplied software on a trial basis, you are responsible for ensuring that it is removed at the specified time or that a licence is purchased prior to the termination of the trial period.

2.2.4 If you need a particular software package or are unsure as to whether you have appropriate licences for the software that you are using, you must consult with INM IT.

2.3 Multimedia, Copyright Protected and Proprietary Data

2.3.1 The company's IT Facilities, including Desktops, laptops, iPads, Tablets, Phones and network file stores, must not be used to copy, store, access or share illegal copyright protected material. Examples of such copyright material would be videos, music, eBooks and games.

2.3.2 **Copyright bypassing tools:** Software tools or utilities which could be used to bypass copyright or licensing restrictions within software or multimedia are expressly forbidden. An example of these tools would be a key generator utility for generating software license keys.

2.3.3 **Non Independent News and Media Confidential Information:** Copying, storing, accessing or sharing non Independent News and Media confidential or proprietary information is strictly forbidden.The Company recognises that information gathering, including confidential information, is an essential function of legitimate journalism journalism and is permitted to the extent necessary for such purposes.

2.4 System Integrity

2.4.1 It is the responsibility of each User to take all reasonable precautions to safeguard the security of the IT facilities and the information contained within them. This includes protecting the IT facilities from physical hazards, preventing unauthorised access to the Company's hardware and systems and only using software approved by INM IT.

2.4.2 The Company has preventative measures in place to prevent suspicious file attachments from entering its computer systems via the Internet. However, the Company depends on all employees to assist in ensuring that its systems are not unduly exposed to viruses, malware or other threats. If you have any doubt about what to do with files provided by clients/customers or other external organisations, contact the IT Helpdesk.

2.4.3 The Company provide secure file storage areas, which are backed up frequently to prevent data loss. You are responsible for ensuring that any Company data for which you are responsible is stored in these secured locations.

2.5 Passwords and Security

2.5.1 You are responsible for the security of your terminal, PC, laptop or other portable device and for protecting any information or other data used and/or stored on these devices. You must not make copies of system configuration for any unauthorised use or to provide to other people/employees for unauthorised uses.

2.5.2 You must not allow your PC/terminal to be used by an unauthorised person. Employees are permitted to share workstations, but only through use of their own assigned authentication credentials.

2.5.3 You must keep your passwords confidential and change them regularly. You must not disclose them to anyone, including INM IT staff. (see appendix 7 A for password policy).

2.5.4 When leaving your PC/terminal unattended or on leaving the office, you must ensure that you log off or lock the system to prevent unauthorised persons using your terminal in your absence. Further, when leaving the office at the end of the working day, laptops should not be left in the office and all Users should carry their laptops along with them in a safe and secure manner.

2.5.5 Upon termination of employment or services, or at the request of the INM IT, any cryptographic information, passwords, keys must be provided to or returned to the Company.

2.5.6 The use of unauthorised remote desktop or desktop sharing software is prohibited. Only software permitted by the Company can be used with approval from the INM IT.

2.5.7 Authentication credentials are not for generic use, or use by more than one person, unless explicitly noted and approved by INM IT.

2.6 Laptops/ portable and handheld computers/remote use

2.6.1 Each User is responsible for the portable computer issued to them and must ensure that the correct procedures are followed, including:

- When accessing the Company's IT facilities remotely, not disclosing your passwords to anyone, for any reason. Do not use log-in scripts which contain passwords or other information of use to hackers.
- Not leaving portable computers and mobile devices unattended and to carry their laptops with them when leaving the office at the end of their working day in a safe and secure manner.
- Storing portable computers in secure cabinets when not in use.
- For employees using portable and handheld computers and mobile devices, being vigilant in public places, as theft is common.
- Not displaying sensitive information in a public place where the screen could be overlooked.
- Not holding Company Data on any unencrypted hard disk, either internal company information or external customer data.

- Using a carrying case to reduce the risk of accidental damage.
- Never allow any unsupervised use of your desktop, laptop or other device whilst it is logged in.
- Never store data on any unencrypted local drive.

2.7 External Storage Media - USB Sticks and External Hard Drives

2.7.1 Employees must not transfer company or customer data to USB sticks, external hard drives, unless there is a necessary business reason to do so. This must be authorised by your line manager and the storage device must be encrypted before any transfer is made.

2.7.2 Employees must not transfer company or customer data to any non-Independent News and Media devices including iPhones, iPads and similar devices. Company and customer data must not be transferred to any Independent News and Media iPhone, iPads or similar device without line management approval which must be given in writing and the storage device must be encrypted.

2.8 Unauthorised Access

2.8.1 To protect the Company's computer systems and records and to preserve confidentiality, access to the Company's IT facilities is controlled. It is imperative to keep all information regarding the business of the Company and the affairs of its clients/customers strictly confidential. Treat electronic information with the same care that you would any written documentation, and ensure that you do not permit any unauthorised person to gain access to the Company's systems.

2.8.2 It is the employee's responsibility to inform the IT Help desk immediately of any actual or suspected system compromise; behaviours or events that you know or suspect breach Independent News and Media IT policies; or actions that could compromise the security of the Company. Indicators which may help you identify unauthorised access would be unusual system behaviour, inexplicable password or software changes, entries in log files you cannot account for, unusual file modification, non-delivery notification or dates and last login times which do not match your last activity.

2.8.3 If you have a legitimate business reason for wishing to access data or programs for which you do not have authorisation, you may only do so with the express authority of your line manager and any other authorisation entities that may be associated with the asset in question e.g. Information Owner, System Owner, and Group Security.

2.8.4 Use of any program, utility or system in connection with any part of the Company's IT facilities designed to:

- Circumvent security measures;
- Determine or identify passwords;
- Breach conditional access systems; or
- Monitor or scan network traffick…

...whether belonging to the Company or to third parties will be treated as a serious disciplinary matter which could lead to dismissal from the Company.

3 Monitoring

3.1.1 The Company places the utmost importance on the protection of Company Data (including, but not limited to, corporate data, customer data and personal data), and the appropriate use of T&I resources. Monitoring will not be directed at specific individuals. All other monitoring will be of a non-directive nature for the purposes outlined in 3.1.2 below.

3.1.2 You should be aware that the Company's IT facilities provide the capability to monitor and log e-mail, voice-mail, Internet and other communications traffic. The Company reserves the right to audit, monitor or record the access, use and content of any communications component of the IT facilities and systems by any User in order to:

- Ensure compliance with this Policy;
- Establish the existence of facts (including for the purposes of conducting disciplinary or grievance investigations or establishing the existence or extent of business agreements, etc.);
- Ascertain or demonstrate standards which are or ought to be achieved (quality control and training);
- Prevent, investigate or detect the commission or potential commission of a breach of this or any other Company policy, a criminal or disciplinary offence;
- Investigate or detect unauthorised or illicit use of the Company's IT facilities and/or systems;
- Secure effective system operation (e.g. to intercept computer viruses or to route traffic); and
- Comply to the extent required by law with requests for access to information by third parties, including regulatory and investigative authorities.

3.1.3 The Company may monitor any communications at any time and use any type of monitoring it deems reasonable.

3.1.4 In respect of monitoring, the Company shall carry out detailed impact assessments to satisfy itself that where monitoring is carried out, the arrangements are justified, proportionate and provide benefit to the company.The Company recognises the fundamental principle of confidentiality of sources and information that underpins our journalism and acknowledges that any monitoring that would undermine that principle should not be undertaken without good cause. Therefore, subject to 3.1.6 below, monitoring can only take place within the Editorial department in accordance with prior 'triple lock' approval which includes the unanimous approval of the Deputy Publisher/Publisher and relevant title Editor. The full details of the triple lock procedure can be found in the Editorial Code of Practice that is available on Indonet.

3.1.5 The triple lock does not apply to monitoring by way of CCTV cameras to ensure that health and safety rules are being complied with, or to check the physical security of the Company's premises and employees.

It also does not apply to ongoing, high level monitoring of suspected security incidents, e.g. attempted logons with incorrect passwords, requests to access the system from suspicious locations.

3.1.6 In respect of high level monitoring of security incidents, in the event of an identified or suspected breach of the Company's IT systems, it will be necessary for the Company to act without delay in order to prevent any unauthorised access to company information or third party data stored on the Company's IT systems. This may require T&I to carry out an examination of a user's internet or email use to identify the nature and extent of any such breach. Any such examination will be limited to such steps as are necessary to identify and mitigate the immediate risks posed.

In the case of Editorial, the examination must be assessed for appropriateness and instigated by the Data Protection Officer who ensures the Publisher and Deputy Publisher are informed and their approvals are in place prior to any action by the Chief Information Officer.

Any further investigation of a user's activity beyond what is necessary to identify and mitigate the immediate risks posed (for example examination of email content) will in all cases require Triple Lock approval.

3.1.7 In the event that any request for monitoring within the Editorial department is submitted for triple lock approval then the following principles shall apply:

i. the person who makes the request must provide the request in writing setting out the reason for the request, providing details of the monitoring that is proposed to be carried out and what it is intended to achieve together with an impact assessment of the proposed monitoring in accordance with Clause 3.1.4;

ii. a request will not be approved unless those considering the request are satisfied that the request has been properly and sufficiently documented in accordance with 3.1.7 (i)

iii. triple lock approval of a request for monitoring within the Editorial department shall not exceed that which is reasonably necessary having regard to the nature of the request;

iv. the Company acknowledges that suspected misuse of one aspect of the Company's IT facilities would not automatically constitute reason to permit monitoring of an employee's entire use of the company's IT facilities. By way of example, suspected misuse of internet access that warrants monitoring of internet use may not automatically justify monitoring of emails or phone logs;

v. those considering the request for triple lock approval will consider whether having regard to all the circumstances the suspected misuse of the Company's IT facilities ~~may~~ ~~have~~ is likely to have occurred in the pursuit of bona fide journalistic purposes, e.g. accessing otherwise unauthorised websites for research purposes. In such an event, the individual concerned ~~may~~ will be given an opportunity to explain the suspected misuse before a monitoring request is approved;

vi. If any member of the Editorial department is intending to access websites that contain or are likely to contain pornography of any kind as part of their work then then they must first notify their Editor.

vii. **UNDER NO CIRCUMSTANCES** should anybody access a website that may contain images of child pornography as part of research for journalistic purposes without the prior approval of the Publisher or Deputy Publisher. Accessing such material is unlawful and sny such request for approval would only be authorised in the most exceptional circumstances and after careful consideration of all relevant information.

viii. Any monitoring carried out on foot of triple lock approval will be notified to the individual concerned as soon it is possible to do so without prejudicing the Company's inquiries or any related disciplinary action.

3.1.8 The Company will appoint an external third party to audit on an annual basis compliance with the triple lock approval mechanism.

3.1.9 Below is a list showing the extent and reason for monitoring which may be carried out by the Company:

- using CCTV cameras to ensure that health and safety rules are being complied with, or to check the physical security of the Company's premises and employees;
- accessing Employees' e-mail accounts or listening to their voice-mails in exceptional circumstances where the Company reasonably believes there is evidence of malpractice or in support of litigation;

- using automated content screening software to determine whether employees are sending or receiving inappropriate communications and to identify the inappropriate use of Company, Customer or personal data;
- examining logs of websites visited to check that individual employees are not viewing or downloading material from Unauthorised Websites (e.g. websites of a sexist, adult oriented, racist or pornographic nature, or websites promoting violence);
- checking logs of telephone numbers called to detect use of premium-rate lines;

3.1.10 The Company reserves the right to add further monitoring purposes where the Company considers it is in its best interest to do so, and/or in order to uphold and maintain the Company's rules and standards.

3.1.11 Where any monitoring is carried out by the Company, this activity is undertaken by authorised personnel only, subject to appropriate safeguards, and compliant with relevant legislation and regulation. Where the monitoring indicates that a potential breach of the Company's rules and standards has occurred, this will be referred to appropriate authorised members of staff for further investigation.

4 ELECTRONIC COMMUNICATIONS

4.1 Introduction

4.1.1 For the purposes of this Policy, the term “email” includes company provided collaboration tools (Skype for Business & Microsoft Teams).

4.1.2 Great care must be taken by all employees in expressing opinions and making judgments using e-mail to avoid causing offence to the recipient either intentionally or not.

4.2 Use of the E-mail System

4.2.1 The e-mail system is the Company’s property. The Company reserves the right to monitor and to access any messages in the system in accordance with the provisions above.

4.2.2 Never send messages that are abusive or which may violate the dignity of a person or create an intimidating, hostile, degrading, humiliating or offensive environment (including, without limitation, any messages that are sexist or of a sexual nature, racist, obscene, abusive or defamatory or which discriminate against another on the grounds of : gender, civil status, family status, sexual orientation, religion, age, disability, race, and membership of the Travelling community).

4.2.3 The Company’s e-mail systems must not be used for unlawful activities (including sending copyrighted materials in violation of copyright laws or license agreements), for solicitation for religious, political, charitable, social or personal purposes, for the purpose of obtaining access to the files or communications of others without a legitimate business purpose or otherwise for the purpose of sending or disclosing messages containing Company confidential or proprietary information to anyone without a right to know.

4.2.4 Improper statements can give rise to legal action against you and/or the Company. They may also give rise to legal obligations – remember that advice given by e-mail may be relied upon and contracts may be created by e-mail. Always remember that e-mail messages, however confidential or damaging, may have to be disclosed in legal proceedings if relevant to the issues.

4.3 E-mail Security

4.3.1 In order to preserve the security of e-mail communications sent externally, encryption may be required in certain circumstances, particularly when sending “Company Confidential” or “Critical” information.

4.3.2 Be aware that employees (within the Company and externally) may delegate to others the ability to read their messages. If your message is of a highly confidential nature, you should avoid the use of e-mail.

4.3.3 The use of auto-forwarding or mail redirection is strictly forbidden. If you are out of the office ensure that “out of office assistant” is turned on before leaving.

4.3.4 The use of 3rd party and external e-mail systems (e.g. Hotmail, Gmail etc) for the storage of Company information, intellectual property or personal information of Company employees is forbidden unless express consent has been provided by INM IT.

4.4 Personal Use of E-mail

4.4.1 Whilst it is accepted that you may need to send personal messages from time to time, you should respect the primary purpose of the e-mail system which is for the business purposes of the Company and keep personal use to a minimum. Personal use of the e-mail system must not create any negative impact on the Company, burden the Company with any significant expense or interfere in any way with employment or other obligations to the Company.

4.4.2 Do not create e-mail congestion by sending trivial messages, forwarding “chain letters”, unnecessarily copying e-mails, or sending large (non-business related) file attachments such as games, screensavers and pictures or external mass mailings.

4.5 Storage of Email

4.5.1 Emails must be stored only within the Corporate Email facility (Office 365), and archiving of emails will be automated through this tool.

4.5.2 You should update your mailbox regularly, deleting unwanted messages and saving important attachments.

5 INTERNET

5.1 Controls

5.1.1 While the Company is committed to use of the Internet for business purposes, suitable controls are required to prevent security breaches or other negative consequences. The networks used for the Internet are not secure and any communications sent by this means can be accessed or modified by unauthorised individuals.

5.1.2 There are also threats from obtaining information from the Internet, virus attachments being the most common. Consequently, Users must adopt procedures which minimise the inherent risks of using the Internet and follow good practice in the way employees behave and the Internet sites that they visit.

5.2 Use of the Internet

5.2.1 The Company has established access to the Internet for specific business purposes. These purposes include the provision of access to information and facilities relevant to the Company's business and the Company's customers and prospects. The Company reserves the right to monitor the IT facilities including use of the Internet for its legitimate business purposes in accordance with above.

5.2.2 Internet activity (including e-mail) is generally grouped into three categories as follows:

5.2.3 **Permitted Business Use:** this includes but is not limited to industry reports, economic information, business news etc.

5.2.4 **Permitted Non-Business Use:** this includes but is not limited to news, weather and responsible brief personal use such as travel information, Internet shopping and social networking/ blogs. Such use must be kept to a minimum, and;

5.2.5 **Misuse:** this includes but is not limited to excessive non-business-related time on-line; accessing large downloads, unauthorised web-logs, games, chat rooms and discussion groups (except as permitted pursuant to below), movies or film clips; advertising personal goods or services; online trading; sending unsolicited e-mail (the practice known as "spamming"); spoofing or defacing any websites; introducing unauthorised software to the system or using illegal software; accessing or using pornographic or adult-orientated websites or e-mails; racist, or sexist websites or e-mails or websites promoting violence.

5.2.6 Disciplinary action may be taken against any employee where usage falls into Section 5.2.5 above.

5.2.7 Employees must not use the IT facilities to access bulletin boards or otherwise post messages on online bulletin boards, websites, or web-logs which do not meet the permitted uses described above, or otherwise which may violate the dignity of a person or create an intimidating, hostile, degrading, humiliating or offensive environment. For the avoidance of doubt, employees must not access sites or post messages of a sexist, racist, obscene, abusive, defamatory, discriminatory or otherwise inappropriate nature. Viewing or downloading pornographic or paedophilic material (which is unlawful) from the Internet is expressly prohibited.

5.2.8 You must not use the IT facilities (otherwise than in the normal course of your employment for the Company) in order to conduct any marketing or sales activities, nor to publish web-logs which may bring the Company into disrepute or which identify the Company and/or its employees whether directly or indirectly.

5.2.9 Where material is obtained from the Internet, you must ensure that any intellectual property rights are respected and in particular that copyright restrictions are obeyed and that virus protection procedures are followed. Where material owned by the Company is published, please ensure that it carries the Company's copyright indications.

5.2.10 The use of peer to peer products and file sharing software is expressly forbidden.

5.2.11 Sensitive Independent News and Media data must not be stored on any personal Internet-based services (Cloud computing), or transferred out of the business using any unauthorised mechanisms or services without approval from INM IT.

5.2.12 The use of **personal** cloud storage, data synchronisation and backup services to synchronise data folders on Laptops/Notebooks/Macbooks such as “Drop Box”, “mobile ME”, “iCloud” and “CrashPlan” are expressly forbidden to ensure that unlicensed or unauthorised software and data are not introduced into Independent News and Media and to ensure that confidential or proprietary information is not inadvertently synchronised to cloud hosting outside of the Independent News and Media agreed cloud provisioned solution.

5.2.13 Bear in mind that whenever you visit an Internet site your identity will be recorded in a “log” by INM systems.

5.3 Mobile Phones and Other Mobile Devices

5.3.1 The Company’s IT facilities include all telephone systems, including mobile telephones and other mobile devices supplied to you by the Company.

This policy applies to all Smartphones with access to Independent News and Media Systems or Corporate Data / email. Smartphone refers to all forms of devices including; iPhone and iPad; Android Devices; Blackberry Devices; Tablet PC (Regardless of Operating System); and Windows Mobile / Windows Phone.

All users should be aware that all access to the Independent News and Media data is subject to controlled monitoring in accordance with Section 3. Independent News and Media reserves the right to review access to ensure compliance with policy, regulatory & legal requirements.

5.3.2 Mobile devices are an asset of The Company and you are responsible for ensuring they are not damaged or defaced, including any external personalisation of the unit. Reasonable wear and tear and accidental damage is accepted, though in the event that this occurs as a result of negligence, the Company reserves the right to pass on any charges incurred for repair or replacement of that unit.

5.3.3 Many services available via Users’ mobile devices, including text messaging and information services, premium phone lines, chat services, downloadable games and ring tones are charged to the mobile phone account. You should not use any such services for non-business purposes, and the Company reserves the right to pass on to you any charges incurred by the Company for unauthorised use.

5.3.4 You must not use your mobile phone whilst driving on Company business, unless you make use of an approved hands-free system.

5.3.5 If you need to use your personal mobile or other mobile device for business purposes you must ensure that the use is permitted on the same basis as that set out in section 5 (Use of the Internet). In addition, the services described in section 5 as “Misuse” shall not constitute legitimate purposes and any charges incurred for such use shall not be recoverable from the Company.

5.4 Termination of Employment / Engagement

5.4.1 Line Managers are responsible for promptly submitting a leaver request through HR to initiate a formal change request informing INM IT following the departure of any User to ensure that access to the Company’s IT facilities is terminated. Similarly, the Human Resources Department has an obligation to inform INM IT following the departure of any employee.

5.4.2 When you cease working for the Company, you are required to return all equipment, computers, hard drives, laptops, iPads, and other Tablets, software, manuals and other IT equipment that has been provided to you to HR on the last day of employment.

5.5 Ownership

5.5.1 All of the IT facilities that you use and any other documents or other products that you may create using the Company's IT facilities, remain the property of the Company. Subject to any applicable laws, this extends to any material or e-mail messages that you may have created or communicated for personal reasons.

5.5.2 All electronic documentation remains the property of the organisation and the organisation reserves the right to retain this information indefinitely. Secure destruction and/or removal of data may be undertaken in line with business requirements.

5.6 Social Media and online usage at Independent News and Media

INM journalists are encouraged to use social media and other digital platforms to help them in their work. At the same time, all staff must abide by the following guidelines. Failure to comply could lead to disciplinary action.

Broad principles of behaviour

When using social media, adhere strictly to the following:

- Do not mix the professional and the personal in ways likely to bring INM or any of its brands into disrepute.
- Do not imply INM or any of its brands endorses your personal views.
- Do not disclose confidential information obtained through work.
- Avoid social media 'spats' or disputes about your own or any other INM articles.
- Do not use vulgar or abusive language when commenting on INM articles or on other people's comments or posts about INM or any of its brands

The following must also be kept in mind:

- Staff journalists at INM must get approval from the Deputy Publisher to start a personal blog, to ensure clear legal and editorial distinction between personal and professional is made.
- Without authorisation, any logos, articles, images or intellectual property of INM cannot be used.
- The use of 'INM' or any such brand reference in your social media account name must only be done with the prior approval of the Deputy Publisher for editorial staff or your senior management representative for non-editorial staff.
- The same journalistic principles of accuracy, tone, and integrity apply on all digital platforms, including social media.
- The same rules of defamation, privacy and contempt apply; observe normal standards of taste.
- Exercise care when sharing, e.g. retweeting, or liking third party social media posts. Never share or like something that you think could be defamatory or a contempt of court.
- Do not assume there is either total security or total privacy; assume everything can be made public.
- INM will not be responsible for anything published by its journalists save that which is published on its print and digital platforms in accordance with the contracted duties of its journalists.
- Journalists contributing to other social networking sites should take careful note of the following:
    - By reading these guidelines, you acknowledge that INM will not bear any responsibility, legal or otherwise, for any material which you choose to publish in a personal manner, either on your own blog or social media account or as a contribution to other online sites and social media.
    - In the event that the Company is named as a defendant in any such litigation, then it reserves the right to seek full indemnity from the individual(s) who chose to publish the material in question and this notice shall be relied upon in that regard.

6 GOVERNANCE

6.1 Enforcement

6.1.1 This Policy must be followed at all times. The Policy applies to all of the Company's IT facilities, whether or not this is attached to the Company network. If you have any queries relating to this Policy, you should discuss this with INM IT.

6.1.2 If you ignore this Policy or misuse the IT facilities available to you, then you will be liable to disciplinary action. The Company reserves the right to withdraw certain facilities (such as Internet access) if these are used in an inappropriate fashion. For breach of any of the rules in this Policy, the Company reserves the right to take all other appropriate disciplinary measures, including where necessary, dismissal of the individual(s) concerned.

6.1.3 This policy is effective immediately.

6.1.4 A current version of this document is available to all members of staff on the corporate intranets.

6.2 Changes to This Policy

6.2.1 The Company may alter this Policy at any time as necessary and where required to reflect changes to the configuration of its systems and applications and to ensure its continued compliance with statutory and other legal requirements.

6.2.2 You will be notified of any material changes to this Policy.

6.3 Health & Safety

6.3.1 It is important that you are able to work safely and that you are not exposed to any unnecessary risks as a result of your work. In particular you should ensure that you are working in an ergonomically safe way and that you take regular breaks from the use of computers during the course of the day. If you have been issued with a laptop, we recommend that you use a separate full-size monitor and keyboard when working in the office, although this is not obligatory.

7 Appendix A Password Policy

7.1 Password Policy

7.1.1 Your user password will be stipulated by the IT Helpdesk Team when your user account is first created. Once you log on for the first time you will be asked to change your password. Your password must meet the following complexity requirements:

- Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Passwords must be a minimum of 8 characters in length.
- Passwords must contain characters from the following categories:
  - English uppercase characters (A through Z).
  - English lowercase characters (a through z).
  - Non-alphabetic characters (for example, !, $, #, %)
- Be changed every 30 days. (You will be prompted to do this automatically)
- Must not repeat any of your previous 4 passwords.

Fifteen days before your password is due to expire you will be asked to provide a new one. You can defer this request for up to fifteen days but on the fourteenth day you will have to provide a new password. Failure to provide a new password will result in exclusion from the network and your inability to access any network resources – including printers, e-mail, network shares.

Users must not disclose their passwords to anyone (including the IT Team) as users are accountable for all activities carried out from with their accounts.

If you enter a wrong password three times your account will become locked out (unable to access the network) and you must contact the IT Helpdesk. If for any reason you are unable to contact the IT Helpdesk your account will unlock after 30 minutes. This is a security feature intended to increase security within the business.

8 ACKNOWLEDGMENT

Your signature attests that you agree to the following terms:

I have received and read the IT Acceptable Use Policy, and I understand and agree to comply with them. I further understand that violation of the policy and/or rules may result in the revocation of computer privileges and may also be subject to further disciplinary and/or legal action.

_____	_____
Employee's Printed Name	Job Title
_____	_____
Employee's Signature	Date

9 Definitions

9.1 Terms

Definition Term	Definition
Company Data	Data relating to Independent News and Media group company customers, employees.
Employee	Employees are defined as anyone working for the Company, whether permanent, temporary, casual, part-time, fixed-term contract and to individuals such as agency staff and consultants and volunteers who are not our employees, but who work at Independent News and Media
IT Facilities	IT Resources together with interface with and use of public networks.
IT Resources	Without limitation, any computer (including laptops and PDAs), server or data network, wireless networks and any telephone handset (including mobile phones), switchboard or voice network provided or supported by the Company
The Company	Any subsidiary of the Independent News and Media Group, not limited to those trading as “Independent News and Media
Unauthorised Websites	Websites of a sexist, adult oriented, racist or pornographic nature, websites promoting violence, that violate the dignity of a person or create an intimidating, hostile, degrading, humiliating or offensive environment, or have content of an obscene, abusive, defamatory, discriminatory or otherwise inappropriate nature.
User	All Company employees and any additional person accessing the Company data, systems, networks or use of the IT Facilities.