IT Security and Social Media Policy	Version:	2.1
	Status:	Final
	Date:	8/1/21

1. Approval Record

Name	Role	Date
Rebecca Clake	Head of People	1/1/20
Tonino Ciuffini	Data Risk Officer	1/5/20

2. Version History

Version	Date	Author	Description (nature of change/update)
V1.0	1/1/20	Rebecca Clake	Initial Creation – Document design
V2.0	1/5/20	Tonino Ciuffini	New paragraphs on Administrators Accounts and Mobile Phone Software
V2.1	8/1/21	Rebecca Clake	Annual review and version control update, added email protocol

3. Related Documents

Document Title	Location	Version Number
Records Management Policy	HR System	V1.1
Data Protection Policy	HR System	V2.1

4. Review and Distribution List

Name	Role	Review Required
Tonino Ciuffini	Data Risk Officer	Contributor/Reviewer
Rebecca Clake	Head of People	Contributor/Reviewer
	All Staff	For Information Only

5. Regulatory Requirements

None

6. Introduction

6.1 Purpose

This policy sets a framework for ensuring due diligence and controls of access to IT systems or equipment on behalf of We are Digital.

6.2 Scope

This policy applies to all members of staff who work under a contract of employment with We are Digital. It also applies to agency staff, contractors, and others employed under a contract of service.

7. Roles and Responsibilities

RACI	Role	Role Holder(s)	Key Responsibilities
Responsible	Process SME	Tonino Ciuffini	• Ensuring process document accurately reflects current practice • Contributing to process changes and improvements, as and when identified
Accountable	Process Owner	Tonino Ciuffini	• Overall ownership and accountability for process definition and execution • Leading change for improving the process • Approval point for any changes/update to the process definition • Ensuring that any changes are properly documented and communicated • Ensuring that ongoing monitoring is in place and carried out
Consulted	Head of People	Rebecca Clake	• Monitoring adherence to agreed process through periodic quality reviews
Informed	All Staff		• Read and accept of document must be completed in HR system • To be included in subcontractor paperwork

8. Instruction

8.1 Overview

These regulations apply to the use of all onsite facilities, and to facilities provided by the Company to its employees for use at home or offsite. Please note that breaches of this policy will be considered as a disciplinary issue resulting in sanctions up to and including dismissal for Gross Misconduct.

Hardware owned, leased, rented or otherwise by We Are Digital employees or third parties approved by the Company may only be directly connected to the network by arrangement with, and with the explicit approval. Such equipment may access the network or other facilities only in accordance with the terms of these regulations.

The facilities may be used only in connection with employees' work for the Company. They must not be used for work of undeclared financial benefit to employees, or the transmission of unsolicited commercial material without the express permission, in writing, of the CEO.

You must read the Data Protection Policy to ensure that you understand your individual and the Company's responsibility with regard to data.

You must not interfere with the work of others or the system itself. The facilities must be used in a responsible manner – in particular, you must not:

- access, store or distribute material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence
- access, store or distribute obscene or indecent material, pornography, etc.
- access, store or distribute defamatory material
- access, store or distribute material such that the copyright of another person is infringed
- use computing equipment or mobile device for playing games
- use computer equipment or mobile device for gambling
- use computer equipment or mobile device for any kind of personal gain (e.g. advertising goods or services)
- gain deliberate unauthorised access to facilities or services accessible via local or national networks or access, store or distribute programmes designed to facilitate such access
- engage in activities which waste resources (your own or other people's time, networks or computers) or which are liable to cause a disruption or denial of service to other users. This includes the following: introduction of viruses into computer systems; use of Internet Relay Chat facilities; use of peer-to-peer networking products; use of internet TV, radio or similar streamed media services; use of social networks such as Facebook, YouTube, LinkedIn, Pinterest and Twitter etc
- engaging in any lobbying or political activity
- engage in any activity that brings the company into disrepute, breach confidentiality or is in any way discriminatory
- use the Company's IT systems to keep a personal "blog"
- engage in activities which are illegal or which might contribute to the commission of an illegal act
- engage in any transaction purporting to be representing the Company when not authorised
- enter into any contract or subscription on the internet on behalf the Company, without specific permission from a senior member of staff

Employees who are authorised users are only permitted to surf the internet for personal and private use, log on to social networking and video sharing websites such as Facebook, Twitter, Instagram and YouTube or use the Company IT systems to keep a personal weblog ('blog') at designated times during the day. The designated times are either before or after normal working hours and during any lunch break. The Company reserves the right to restrict access to social networking and video sharing websites at any time.

The Company's IT and communication resources are valuable and expensive business resources and must be treated with care and respect, you must not:

- Modify or attempt to fix any of the Company's IT and communication resources. Any fault should be reported immediately to the Head of People
- Download or install any programme, software or screensaver onto the Company's IT equipment or mobile device
- Copy, modify, transfer or remove any of the Company's software, data or resources

We are guardians of considerable amounts of sensitive data, and it is vital for our business integrity that care is taken to safeguard both the information and the database systems themselves.

8.2 Computer and Password Rules and Management

You must not gain unauthorised access to or violate the privacy of other people's files, corrupt or destroy other people's data or disrupt the work of other people.

You are responsible for the security of your computer terminal (whether desktop or laptop) or mobile device and must not allow the terminal to be used by anyone not employed by the Company.

You will be issued with a login ID and password. You must keep these secure and you must not disclose them to anyone else. You must not:

- permit anyone else to use your login ID or password
- use any other person's login ID or password
- change your login ID or password unless otherwise instructed by your Manager

If you leave your workstation for any period of time you should take appropriate action and, in particular, you should log off and/or set your screen saver with an appropriate password.

It is your responsibility to prevent inappropriate access to your files. Your password must be kept safe and not be disclosed to anyone.

Passwords should be complex and not contain personal information or things that are easily linked to you through information readily available on the web. Best practice is to select 3 random words and include upper and lower case, numbers and symbols in the combination.

Passwords should be updated every 90 days where appropriate and when changing they should be substantially different from the previous one.

As far as possible We Are Digital will minimise the use of administrator accounts by We Are Digital staff for our core IT network and PCs. We will rely on these facilities to be managed by our IT providers and ask them to manage and use the administrator accounts on our behalf. This is to reflect the additional technical knowledge required to operate these accounts, and the additional controls and logging of events that this provides.

If an administrator account is required to be used by a We Are Digital member of staff, then this must be approved by ELT. This should be following the submission of a clear reason for why administrator access is required and the requested scope of use e.g. installing software, making configuration changes. Should an approved requirement cease to exist then the administrator account access should be revoked. Any administrator account access approvals should be reviewed annually as a minimum.

Following the approval of administrator account access then the member of staff with administrator access:-

- Must only be use it for administration activities approved when it was requested
- Must never use the account for general activities e.g. accessing e-mail or web browsing
- Must never reveal the administrator password to other staff, if it is it revealed it must be changed immediately
- Record in a formal log all administration activities carried out using the administrator account

8.3 Email Policy

The use of the e-mail system for business purposes within the Company is encouraged, as it facilitates communication and improves efficiency. Used correctly, it is a facility that is of assistance to staff, customers, consultants and suppliers. Inappropriate use, however, can cause many problems, ranging from minor distractions to legal claims against the Company. The Company reserves the right to monitor the use of email.

Personal use of the company e-mail system is permitted provided that it is not excessive and does not interfere with the performance of your duties or distract others from their duties.

Your work email account must not be used:

- for the transmission of unsolicited commercial or advertising material, chain letters, press releases, jokes, or other junk-mail of any kind
- for the transmission of any pictures, video or sound files unless for business purposes
- knowingly for the transmission of any file that contains a virus or malicious programme code which could inhibit, damage or destroy the recipients IT software, systems and/or equipment

and you must not:

- Under any circumstances send or disclose any colleague, client or customer personal data to any personal email addresses including your own
- Transfer any personal data within the main body of a business email. Personal data should be encrypted or sent in a password protected format as an attachment to an email
- Send or forward emails containing anything which may be considered offensive or harassing including discrimination against others based on their race, gender reassignment, sex, pregnancy or maternity, sexual orientation, age, disability, religious or political beliefs, marital or civil partnership status
- Send or forward sexually oriented emails or images
- Send potentially defamatory emails
- Send unnecessary or trivial emails such as jokes or gossip

All correspondence by email should contain the Company's disclaimer.

If you receive any of the above from an internal source, you should raise the issue with your Line Manager. If not, immediately delete the email.

It is absolutely essential that you do not open emails or attachments from non-trusted sources, as it is easy for viruses to enter the network. If you have any doubts about the source or content of an email, do not open it. Contact the Data Risk Officer or IT provider and allow them to assess the email.

Content and Style of Emails

Emails tend to be treated more informally than other written correspondence. However, emails form a permanent record of any correspondence and nothing should be put in an email which you would not be prepared to put on an internal memorandum or on Company headed notepaper. Review each email carefully before sending it.

Emails must never contain anything unprofessional or that could damage the Company's reputation. You should not refer to anyone (either internally or externally) in an email in a way that you would not want them to read.

You must not send electronic mail which is irresponsible, or likely to cause offence, or use network messaging without authority. “Irresponsible” use includes unsolicited postings to large numbers of people or indiscriminate postings.

Protocols	Requirements
Purpose of Email	• Ask Why and what is the Purpose for this email • Pick up the phone or go to see that person first
Work Life Balance	• No emails to be sent outside of the 8am to 6pm window and none to be sent at weekends or on public holidays • Park as drafts and send out the next working day

Email Structure and Content	• Subject Line must align with the content and actions
	• Executive summary structure and contents
	  ○ Succinct explanation – 1 line only
	  ○ Bullet points
	  ○ Actions and next steps must be specific, measurable, achievable, realistic and time-bound
	• Review and check content before sending
	• Check that the addressees are correct

Reducing Emails	• Use catch-ups to reduce use of emails • Think twice before using CC
Confidentiality	• Where sending the same communication to multiple individuals and using a non WAD email address i.e trainers, job applicants, learners; you MUST ensure that you use the BCC function rather than the to function to protect the privacy of their personal email account details

8.4 Internet Policy

Personal use of the Company's Internet is permitted outside of your normal working time. Personal use during your designated breaks is limited. But you are strictly prohibited from accessing, downloading or viewing any site which may:

- contain pornographic, obscene or offensive material
- contain discriminatory, religious or political material
- promote criminal or unlawful activities
- be threatening, abusive, libellous or defamatory
- encourages conduct that would constitute a criminal offence, give rise to civil liability, otherwise violate any local, national or international law
- infringe copyright and/or other intellectual property rights of people or companies, including, but not limited to software programs protected by copyright or material produced by someone else
- Require a TV licence to be held to view such as iplayer, ITV hub etc

You must not download any software from the Internet without the authorisation of your manager or the Data Risk Officer.

Never use the Internet to transmit confidential personal or business sensitive information.
The organisation reserves the right to monitor employees' internet and IT usage, whenever you use the company's resources and systems, you give the company consent to monitor your activities.

8.5 Mobile Device Policy

The Company recognises that there is a need to provide selected individuals with mobile devices to enable them to complete their role responsibilities. Where the role is identified as requiring the mobile device the equipment will be ordered by the Head of People as part of their induction process.

Under no circumstances should any staff link their work account details to their own personal mobile device or equipment. This is due to concerns over cyber security and malware configuration on these devices. Failure to observe this may result in disciplinary action being taken.

Company devices should be protected by either a 8 digit code, fingerprint or face recognition or a combination of both.

Staff members who have access to a Company mobile device are responsible for ensuring that the device is regularly updated and is running the most current version. This is to protect against cyber security risks.

Where Company Equipment is no longer able to support the current update version then the staff member must request a replacement by completing the equipment replacement request form and submitting to the Head of People.

Company Mobile devices are only to be used for the purposes of business use.

Staff should only use the following software and apps on mobile phones and devices supplied by We Are Digital:-

- Software and apps that come pre-installed on the phone
- Software and apps on the We Are Digital approved product list
- Even then generic software and apps must be installed from the Apple App Store, Google Play Store or Samsung App Store

Staff can request that products are added to the approved product list by submitting the Request for New Mobile Device App Form to the Data Risk Officer. The form must outline the reason why the application should be used on a We Are Digital device and the business benefits that will be achieved. The Data Risk Officer will investigate the product and decide within one working week as to whether the application is approved for use. If the application is not approved, staff can appeal to the Chief Operating Officer to ask for the decision to be reviewed.

8.6 Social Media Policy

Social media is an interactive online media that allows users to communicate instantly with each other or to share data in a public forum. It includes social and business networking websites such as Facebook, Twitter and LinkedIn. Social media also covers video and image sharing websites such as YouTube and Flickr, as well as personal weblogs ("blogs"). This is a constantly changing area with new websites being launched on a regular basis and therefore this list is not exhaustive.

This policy applies in relation to any social media that employees may use.

Use of Social Media at Work

Employees are only permitted to log on to social media websites or to keep a personal weblog ("blog") using the Company's IT systems and equipment outside their normal working hours (for example, during lunch breaks or before the working day has started or after the working day has finished) and this must not under any circumstances interfere with their job duties or have a detrimental effect on their productivity. This includes laptop and hand-held computers or devices distributed by the Company for work purposes. The Company nevertheless reserves the right to restrict access to any of these types of websites at any time. Where employees have their own computers or devices, such as laptops and hand-held devices, again they must limit their use of social media on their own equipment to outside their normal working hours.

However, employees may be asked to contribute to the Company's own social media activities during normal working hours, for example by writing Company blogs or newsfeeds or managing a Facebook account or running an official Twitter or LinkedIn account for the Company. Employees must be aware at all times that, while contributing to the Company's social media activities, they are representing the Company.

Company's Social Media Activities

Where employees are authorised to contribute to the Company's own social media activities as part of their job duties, for example for marketing, promotional and recruitment purposes, they must adhere to the following rules:

- Use the same safeguards as they would with any other type of communication about the Company that is in the public arena.
- Ensure that any communication has a purpose and a benefit for the Company.
- Obtain permission from their line manager before embarking on a public campaign using social media.
- Request their line manager to check and approve content before it is published online.
- Follow any additional guidelines given by the Company from time to time.

The social media rules set out below also apply as appropriate.

Social Media Rules

The Company recognises that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the Company in these circumstances, employees must be aware that they can still cause damage to the Company if they are recognised online as being one of its employees. Therefore, it is important that the Company has strict social media rules in place to protect its position.

When logging on to and using social media websites and blogs at any time, including personal use on non-Company computers outside the workplace and outside normal working hours, employees must not:

- Other than in relation to the Company's own social media activities or other than where expressly permitted by the Company for business networking websites such as LinkedIn, publicly identify themselves as working for the Company, make reference to the Company or provide information from which others can ascertain the name of the Company.
- Other than in relation to the Company's own social media activities or other than where expressly permitted by the Company for business networking websites such as LinkedIn, write about their work for the Company – and, in postings that could be linked to the Company, they must also ensure that any personal views expressed are clearly stated to be theirs alone and do not represent those of the Company.
- Conduct themselves in a way that is potentially detrimental to the Company or brings the Company or its employees, clients, customers, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content.
- Other than in relation to the Company's own social media activities or other than where expressly permitted by the Company for business networking websites such as LinkedIn, use their work e-mail address when registering on such sites or provide any link to the Company's website.
- Allow their interaction on these websites or blogs to damage working relationships with or between employees and clients, customers, contractors or suppliers of the Company, for example by criticising or arguing with such persons.
- Include personal information or data about the Company's employees, clients, customers, contractors or suppliers without their express consent (an employee may still be liable even if employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable) – this could constitute a breach of the General Data Protection Regulations (GDPR) which is a criminal offence.
- Make any derogatory, offensive, adverse, discriminatory, untrue, negative, critical or defamatory comments about the Company, its employees, clients, customers, contractors or suppliers, or any comments which might reasonably be considered to insult, damage or impugn the Company's or their reputation or character (an employee may still be liable even if the Company, its employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable).
- Make any comments about the Company's employees that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying – employees can be personally liable for their actions under the legislation.
- Disclose any trade secrets or confidential, proprietary or sensitive information belonging to the Company, its employees, clients, customers, contractors or suppliers or any information which could be used by one or more of the Company's competitors, for example information about the Company's work, its products and services, technical developments, deals that it is doing, future business plans and staff morale.
- Breach copyright or any other proprietary interest belonging to the Company, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work – if employees wish to post images, photographs or videos of their work colleagues or clients, customers,

contractors or suppliers on their online profile, they should first obtain the other party's express permission to do so.

Employees must remove any offending content immediately if they are asked to do so by the Company.

Work and business contacts made during the course of employment through social media websites and which are added to personal social networking accounts amount to confidential information belonging to the Company and accordingly the Company may ask for them to be surrendered on termination of employment.

Employees should also ensure that on termination of employment they update their social media profiles to reflect the fact that they are no longer employed by We Are Digital.

Employees should remember that social media websites are a public forum, even if they have set their account privacy settings at a restricted access or "friends only" level, and therefore they should not assume that their entries on any website will remain private or confidential.

Employees must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for example by setting their privacy settings at a high level and restricting the amount of personal information they give out, such as date and place of birth, schools attended, family names and favourite football team. This information may form the basis of security questions and/or passwords on other websites, such as online banking.

Should employees observe inaccurate information about the Company on any web sources of information, they should report this to their line manager in the first instance.

Social Media References

Where employees (or ex-employees) have set up personal profiles on business networking websites such as LinkedIn, these websites may include the facility for the user to request their contacts or other users to provide them with open recommendations, endorsements or references which are then published on their personal profile web pages for other contacts or connections, or prospective contacts or connections, to read. As these could potentially be construed as open references given on behalf of the Company, employees are prohibited from providing these types of recommendations, endorsements or references online to or for the benefit of other employees or ex-employees without the prior permission of their line manager.

If these types of recommendations, endorsements or references are requested online by clients, customers, contractors, suppliers or other Company-related business connections, employees should refer such requests to their line managers.

Social Media Monitoring

The Company reserves the right to monitor employees' use of social media on the internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- Promote productivity and efficiency.
- Ensure the security of the system and its effective operation.

- Ensure there is no unauthorised use of the Company's time, for example to check that an employee has not been spending an excessive amount of time using social media websites for non-work related activity when they should be working.
- Ensure that inappropriate, restricted or blocked websites are not being accessed by employees.
- Ensure that all employees are being treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to harassment contrary to the Equality Act 2010.
- Ensure there is no breach of commercial confidentiality.

The Company reserves the right to restrict, deny or remove internet access, or access to particular social media websites, to or from any employee.

Contravention of this Policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the Company's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

9. Quality Control Log

No	Risk/Issue	Control	Control in Place Y/N
1	Inconsistent execution of the process by different people / departments	Training on the policy to take place as part of induction process and annual refresher training to take place	Y

10. Glossary

Term	Description