Videndum

IT Policy

Videndum PLC

19 December 2022

Contents

IT Policy
(“the Policy”)

Section 1 – Purpose and confirmation statement

Scope of the Policy

The purpose of this Policy is to ensure that all employees and contractors are aware of Videndum rules with regard to the following:

- The use of Company supplied computer technology and services;
- The use of electronic communication such as E-Mail and Instant Messaging;
- The use of social media platforms such as Facebook and Twitter, either internal or external to the business;
- The management of personal data.

Any third parties such as visitors, agents or consultants using Videndum’s computer network and services are also subject to compliance with this policy. It is the **responsibility of the employee** who authorises the third party use to ensure that the third parties have read and understood the terms of this policy and agree to be bound by it. Where the policy refers to employees it is inferred that it also refers to contractors.

The Policy has been implemented to protect Videndum and employees’ reputations and to ensure a secure, trusted and safe computing environment for all our users. Employees deemed to be in breach of the Policy may be subject to disciplinary procedures ranging from (but not limited to) verbal warnings to instant dismissal, and may be subject to either civil or criminal penalties under the applicable legislation.

Confirmation statement

Your signature on this document indicates that you have read, understood and agree to abide by the rules set out in this Policy. In particular, you agree to the following:

- Personal use of Videndum IT network and resources should be limited and reasonable and should not affect the employees’ duties;
- You shall not access websites which contain obscene, pornographic, racial, sexual, political or other material contrary to Videndum policies and values; All data (personal, confidential, sensitive) should be protected and carefully handled and communicated; All IT equipment should be carefully secured and laptops should be locked away at night; Any IT breaches including loss of data and loss of IT equipment must be reported immediately;Software should not be downloaded and used without the express authorisation of IT; All forms of electronic communications must be conducted in a professional manner, in compliance with Videndum’s Code of Conduct and the guidelines outlined in the Policy.

Please sign and return this page to your local HR contact.

I have read and understood the terms and conditions laid out in this document and I accept the responsibilities required of me therein.

Failure to return this document to your local HR contact may result in your user account being locked out.

Name	
Employing Company	
Date	
Signature	

Section 2 – General Principles of computer use

Employees and contractors should be aware of the rules in using any computer service supplied by the Videndum.

Prohibited activities

In conjunction with the rules regarding the use of electronic communications (section 3), employees should be aware of the rules in using any computer service supplied by Videndum. Employees must respect the confidentiality of information stored within Videndum IT systems and the integrity of the overall computing environment, ensuring that they do nothing to damage, or potentially damage, the integrity or disrupt the intended use of the systems.

The following activities are strictly prohibited:

- It is a disciplinary offence to attempt or gain unauthorised access to Videndum's IT services without authority to do so, or to disrupt the intended use of the Videndums computer system or network resources.
- The unauthorised removal or extraction of files to or on any server in Videndum's network.
- Those which may disrupt the intended use of the Videndums computer system or network resources.
- The unauthorised use or copying of proprietary software or copyright material (see section 3 on software use).
- Accessing or attempting to access any internet sites which:
    - Are obscene;
    - Contain racial, sexual, political or other hate material likely to cause offence;
    - Display pornographic images;
    - Contain offensive language;
    - Any purpose which is illegal or against Videndum's policy or contrary to Videndum's interest.

Personal use of Videndum network and services is not strictly prohibited but it should be limited and reasonable and should not adversely affect the performance of the employee's duties. You should never use Videndum's network and services to access pornographic, betting, or other sites which are deemed controversial. Not only is this a violation of Videndum policy, but it also increases the risk that malware or viruses will infiltrate our network.

Personal e-mail must be clearly marked as such either by the means of applying a category or placing into an appropriately named folder. Never use your personal email account to send a work-related email.

Employee preventive measures

Employees should be mindful that Videndum's systems contain confidential information and that unsolicited approaches may be made by third parties in an attempt to gain access to company information (also known as phishing). Employees should be vigilant when answering the phone or replying to emails and should not divulge company or personal information unless they are certain it is to a reputable and known party. Any suspicious or unusual emails should be reported to your local IT Department. Employees responsible for making payments must never deviate from the established payments protocol.

IT systems and firewalls alone cannot prevent and detect the many types of external malware and virus infections. You should not open work-related or private emails or attachments from your work computer which are from unknown sources as these could contain viruses which might infiltrate our network. You must be extremely wary of any email URL links or pop ups which require you to enter credentials.

Ensure that you action all IT requests such as anti-virus software updates / password changes immediately. If you become aware that your device(s) are infected, you must notify your IT Department immediately.

You should never write down or share your password, whether your direct peers or the IT department. In the event of IT requiring access another procedure will be followed to provide support and assistance. You must adhere to the Videndum's access control guidelines as contained in the Access Control policy.

Rules on Bring Your Own Device (BYOD)

BYOD for work purposes is generally prohibited because of the implications for data integrity and IT security. Any use of personal equipment for work purposes must be expressly cleared with your IT department. This covers all electronic devices including but not limited to PCs, laptops, tablets and mobile phones.

Exceptions can be made if suitable security measures and access controls are implemented by the IT Department, and necessary control methods put into place.

Safeguarding equipment

It is the employee's responsibility to ensure the security and integrity of any Videndum computer or communication equipment. This includes, but is not limited to, desktop computers, laptops, modems, printers, tablets and phones.

Users of personal computers, laptops and tablet devices are also reminded that they should safeguard their systems by "locking" their desktops (with a password) when away from their desks. This applies regardless of the length of time you expect to be away from your desk. When leaving the office each day computers must be turned off and not left on stand-by overnight.

Laptops must be locked away overnight (if on a Videndum premise), or secured with a locking system, and must be in your possession at all times when travelling. Never check-in a laptop unless required by law, and never leave a laptop in a vehicle if the vehicle is unattended.

The loss of any Videndum equipment should be reported to your local IT Department immediately.

Use of removable devices

Employees should be aware of the origin of such devices and should not insert an unknown device into a Videndum laptop or computer without it being scanned for viruses. You should contact your local IT helpdesk if you have any concerns about using devices in your possession.

Employees must not use removable data storage devices to extract Videndum information for their own personal use or commercial gain. Doing so would be a breach of the Code of Conduct and could lead to disciplinary action or immediate dismissal.

Only encrypted devices should be used.

Use of external file sharing facilities

The use of file sharing facilities outside of the companies' control, for storing important information is strongly discouraged unless the use and access to the relevant solution is controlled by the IT Department. Intellectual property or personal data should never be stored in external facilities unless controls are in place to ensure its security and integrity.

Protecting data

You must have a clear understanding of the nature and sensitivity of any data that is in your possession or that you have access to. This may include: confidential payroll or customer information, intellectual property such as commercial drawings, commercially sensitive information such as pricing, or credit card information.

All files containing sensitive information, and the communication thereof, should be suitably protected and encrypted. More details can be found in the Data Protection policy.

The download of company information for personal gain is strictly forbidden and may lead to prosecution.

You must ensure that all data/information in your possession is regularly backed-up. All data should be archived in accordance with your local policy.

See section 5 regarding guidelines specific to personal data, and please refer to your business unit's record retention policy.

Section 3 – Software use

Videndum has multiple agreements in place for the purchase of standard desktop software (for example Microsoft Office) and all software must be procured with prior written approval from your local IT Department. Users must not knowingly download software without prior approval from your local IT Department. Exceptions to this are users working in a software development capacity, who may download drivers and/or patches as part Videndum's related development work. The IT Teams have a right to audit IT systems and devices used by employees.

Software duplication or transmission

Users may not duplicate any licensed software or related documentation for use either on Videndum's premises or elsewhere unless Videndum has been expressly authorised in advance to do so by agreement with the licensor. A duplication of licensed software is a breach of the license agreement and will lead to financial penalties for Videndum.

Users may not give software to any third party. Videndum employees may use software on the local area network or on multiple machines only in accordance with applicable license agreements.

Transfer of software licenses

No user may sell, lend, sublicense, transmit, distribute, give or otherwise convey or make available software or interest therein to any unauthorised individual or entity without permission from your local IT Department.

Software de-compilation

No user may de-compile, reverse engineer or disassemble software unless permission has been explicitly granted in advance by the software copyright owner.

Software Installation or Removal

Only members of your local IT Department or authorised users are allowed to install or uninstall software on personal computers and servers. This includes, but is not limited to, commercial software, shareware software and freeware software.

Videndum developed software may be installed by individuals but only after prior (written or email) approval from your local IT Department.

Personal software may be installed with prior (written or email) approval from your local IT Department. Your local IT Department may ask for proof of ownership if software is installed on Group equipment. All software license information must be logged with your local IT Department.

Software Registration

When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of the company and department in which it will be used. Software must never be registered in the name of the individual user.

Software Licensing

Your local IT Department shall keep all original copies of licenses for all software used within Videndum.

Apps

You may download apps to your work mobile phone or tablet that are either work related or assist you in performing your work. Examples of non-work-related apps which you may download may include LinkedIn, travel apps, news apps, banking etc. The cost of work-related apps can be claimed via expenses if they have been authorised by your IT department and line manager in advance. All other apps must be paid for by the employee. You should avoid downloading apps to your work mobile phone or tablet which are unrelated to your job, or which may impact your job, or the security or integrity of the company.

Copyrights

Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and may not copy, download, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner (see section on software use).

Section 4: electronic communication

This part of the policy outlines Videndum's rules with regard to the acceptable use of electronic communications.

The following rules apply to all electronic communications including but not limited to e-mail, twitter, instant messaging and text messaging that are accessed using Videndum computer equipment or via Videndum's paid access methods, or used in a manner which identifies the individual within Videndum

Inappropriate content or use

The list outlined below is merely indicative and not exhaustive of conduct that may result in disciplinary proceedings. Employees should be aware that Videndum' may inform the appropriate authorities if, for instance, there has been a criminal offence or breach of data protection legislation or Videndum' believes an offence may be likely to be committed. Electronic media may not be used for knowingly transmitting or storing any communications or information that:

- Is of a discriminatory or harassing nature;
- Is derogatory to any individual or group or otherwise could bring Videndum or its employees into disrepute;
- Is obscene or X-rated, or which pose a risk to Videndum that they may be regarded as such and, in particular, pornographic material must not be received, stored or distributed either internally or externally;
- Is of a defamatory or threatening nature; and/or
- Is a "chain letter", junk or spam e-mail.

Electronic Communication and Legal Liability

Employees should be aware that the legal responsibility for employee written e-mails and indeed for any Internet misuse by an employee rest with both the Company and the individual(s) responsible. There is a general perception that electronic communication is an informal form of communication and that it is not legally binding, however, employees should be aware that this is not always the case, and in certain circumstances there may be a legal liability.

Electronic communication can be the equivalent to issuing a letter on the Company's letterhead and, for the avoidance of doubt, employees should be aware that this type of communication may be capable of forming or varying a contract. Employees should, therefore, assume that electronic communications are legally binding on the Company and should take the same degree of care in relation to this type of correspondence (both external and internal) as they would in relation to formal correspondence on Company letterhead. You should not enter into any form of contract or initiate any purchase or sale electronically on behalf of the Company unless and until all normal authorisation procedures have been complied with (for example Videndum's Delegated Powers and Levels of Authority).

Please be aware that when using e-mail communication, you must use the correct email signatures that have been issued by Videndum or your Division. This is a legal requirement. Please contact the Videndum Head Office or your Divisional Marketing Director should you need confirmation of the correct format of your email signature.

Guidelines for Electronic Communications

Good communication should involve talking to your colleagues, suppliers and customers. Often issues can be resolved much more quickly and with less chance of misinterpretation. However, where an email is a more appropriate form of communication both internally and externally, for example when a supporting document and explanation is required, the following guidelines should be followed.

E-mail communications in particular are often perceived as being closer to informal speech rather than formal writing. **Messages can be sent quickly and often with little thought regarding their** contents. In addition, e-mail and instant messaging is increasingly the principal form of tangible contact between Videndum and its customers and/or suppliers and, as a result, it may have a fundamental impact on their impression of Videndum. In order to minimise offensive or harassing communication and to protect Videndum's reputation the following guidelines must be adhered to:

- The inappropriate use of upper case in electronic communication is generally interpreted as SHOUTING and should be avoided;
- The subject field in e-mails should contain a meaningful description of the content of the e-mail and e-mails should only be sent to persons who need to see the e-mail;
- Electronic communication should be written in an appropriate tone using normal business language reflecting the standards normally adopted for letter headed paper correspondence;
- Employees must not abuse others or write derogatory comments even in response to abuse directed at them;
- If a user receives an e-mail or electronic communication in error, they must inform the sender immediately and delete the message from their mailbox or conversation history;
- E-mails must include the appropriate legal information such as Company name and registration number. Templates have been issued by the Group and must be used; Check the recipients' names and email addresses carefully.
- Make sure you have correctly selected Reply or Reply All, and that everyone is authorised to read the information.
- When forwarding or replying to an email, make sure all of the content and attachments are appropriate to be sent to the recipients.
- Never set up an automatic forward to another email address.

Electronic Communication Monitoring

There is a general expectation that all correspondence via e-mail is secure and private. However, Videndum, for legitimate business purposes, may monitor electronic information created, stored and/or communicated by an employee, though Videndum attempts to respect the individual's privacy within the terms of this policy. The following should be noted:

- Videndum routinely monitors usage patterns for both voice and data communications (for example the number called or web site accessed, call lengths, frequency of calls etc.). This type of monitoring allows Videndum to perform accurate cost analysis, better financial allocations and to actively manage the systems required to provide the various technology services.
- Videndum reserves the right, in its discretion, to review any employee's electronic files and messages (email/Instant Messaging History) and usage to the extent necessary to ensure that Videndum provided services are being used in compliance with the law, to protect Videndum reputation and to protect the stability of Videndum computing environment.

Employees should, therefore, not assume electronic communications are totally private and confidential and should transmit highly sensitive and/or personal information in other ways. Employees considering sending or receiving personal information via e-mail or instant messaging systems should consider using a private e-mail service external to Videndum's.

Personal use is at the discretion of Videndum, and employees found to be abusing these facilities may have their rights removed.

Employees on holiday or who have left the Company may have their e-mail mailboxes or instant messaging conversation history files opened and searched for business related communications. With regards to personal privacy as listed within the Human Rights Act (1988), communications which are clearly of a personal nature will not be accessed or disclosed by Videndum.

E-mail and Instant Messaging Housekeeping

Employees are encouraged to practice good housekeeping with regard to e-mail and/or instant messaging services, especially given that individual storage space restrictions are in place. It is the employee's responsibility to store only items that may be required for retrospective access. It is recommended that frequent archiving of emails is carried out and the data placed on a network drive that is subject to regular backup. Users who require guidance in performing housekeeping duties should contact your local IT Helpdesk to arrange for training.

Social Media communication

The use of Social media websites and applications has expanded dramatically over the last few years. This form of electronic communication can be a concern for employers and employees in that it:

- Has the potential of being instantly and universally publicised or disseminated
- Has the potential to be communicated to a much wider audience than originally intended
- Has the potential to be irrevocable

While Videndum does not, in any way, seek to impose its view of the "proper" use of these forms of communication on any of our employees, the fact is that where we, as employees, are either speaking of matters involving our work or are identified as representing the Group, it is easy for a reader of a Facebook page, a Twitter tweet, your Linked In profile or an email to identify what is being said as being a position of Videndum for whom you work. It is not acceptable to mention any sensitive Bibendum information, or statements regarding, but not limited to: acquisitions, contracts wins/losses, negotiations, employees, internal policies, movements, plans or designs. Only fact-based information may be acceptable and not subjective comments / opinions.

The detailed rules which must be adhered to are highlighted in the Code of Conduct (Social Media policy section).

Section 5: Personal Data

For more information, please refer to the Personal Data protection policy. Below are some of the key provisions.

Managing personal data
Personal data applies to data in any format that may directly or indirectly identify a natural person. This data takes many forms, including, but not at all limited to: a name, a postal address, a birthdate, email address or even an IP address. Any personal data which you are handling needs to be treated with great care. Most importantly it must have been obtained for a legally valid purpose and with the person's consent. It needs to be kept safe and secure – this includes hard/soft copy files and documents.
When communicating personal data ensure that you restrict what is being sent to only what is necessary. In addition, any personal data sent should be encrypted by any practical means.

When there is no longer a legitimate reason for keeping personal data, it should be deleted. This includes any emails containing personal data. You may at any point be required to clearly identify any personal data which you hold, where this is held, and the rationale for maintaining such information.

IT Security incidents and breaches

If you become aware of an actual or potential data breach, or other IT Incidents, you must immediately notify your IT Department and Line Manager, who will notify the nominated Data Protection Lead and the Group's Company Secretary. They will assess and initiate next steps and remedial actions.

Immediate reporting of any issues, even if not confirmed, must be done immediately in order for Videndum to assess the need for reporting to the relevant data protection authorities (within the EU and UK, this must take place within 72 hours of discovery.

Failure to comply with these timeframes may result in the Group incurring significant fines.

"Subject Access" Requests
Any individual (Data Subject) has a legal right under European data protection law to be informed whether personal data is processed (which includes being held or stored); a description of the data held; the purposes for which it is processed and to whom the data may be disclosed; a copy of the information constituting the data; and information as to the source of the data. This must be provided by the Group within 30 days of the request date.

If you receive a Data Subject access request, you must immediately pass this on to your responsible Data Protection Lead who will coordinate the response, confirm the identity of the data subject and start a log/tracking sheet detailing the date the request was received and when each stage of the request was completed.

The Data Protection Lead will contact all holders of data (i.e. the relevant Departmental or functional lead) to search for both manual and electronic information. The registered holder will be responsible for checking systems (including computer held records), emails and files for any reference, directly or indirectly, relating to the Data Subject.

Third parties (data processors)
In many cases we transfer personal data to a third party which we then refer to as a "Data Processor". This includes our outsourced payroll providers, Pensions providers, digital marketing providers and any other company which is entrusted with personal data.
If you are responsible for a contractual relationship with a Data Processor, you must ensure that adequate safeguards are in place to ensure that the data is safely looked after. Your Data Protection Lead will be able to advise on the arrangements including contract terms to put in place.

Section 6 – Contracts and References

Data Protection Leads

Group, European Services and Production Solutions: Ben Skinner

Media Solutions: Roman Contin

Creative Solutions: Carel Van Heerden

How to contact your helpdesk

Your Business Unit	How to contact your IT Helpdesk	
Group	helpdesk@videndum.com	+44 (0) 1284776700
Creative Solutions	https://app.getguru.com/card/TapqapMc/IT-Support-Requests-Contacting-IT-for-Help	
Media Solutions	https://videndummedia.atlassian.net/	Federico Soster:+39 0424 555 854 Valentina Pasquali:+39 0424 555 890
Production Solutions	helpdesk@videndum.com	+44 (0) 1284776700